PATENT APPLICATION SERIAL NO. ____________________

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

```
10/26/2000 FFANAEIA 00000028 09694416

01 FC:108-                        710.00 OP
02 FC:110                         864.00 OP
03 FC:109                         960.00 OP
```

```
Repln. Ref: 11/07/2000 KHARLING 0010022100
DA#:023964    Name/Number:09694416
FC: 704                          $126.00 CR
```

```
Adjustment date: 11/07/2000  KHARLING
10/26/2000 FFANAEIA 00000028 09694416
02 FC:110                        -864.00 OP
```

```
11/07/2000 KHARLING 00000048 09694416

01 FC:110                          738.00 OP
```

PTO-1556
(5/87)

*U.S. GPO 1999-459-082/19144

10-24-00

A1 Res

PTO/SB/50 (08-00)
Approved for use through 12/30/2000. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REISSUE PATENT APPLICATION TRANSMITTAL

Addressed to:

Assistant Commissioner for Patents
Box: Reissue
Washington, DC 20231

Docket No.	20206-014(PT-TA-410)
First Named Inventor	COLLINS
Original Patent No.	5,848,159
Original Patent Date	December 8, 1998
Express Mail No.	

APPLICATION FOR REISSUE OF: ☒ Utility Patent ☐ Design Patent ☐ Plant Patent

APPLICATION ELEMENTS (37 CFR 1.173)

1. ☒ Fee Transmittal Form (PTO/SB/56)
2. ☐ Applicant claims small entity status. See CFR 37 1.27.
3. ☒ Specification and Claims in double column copy of patent format (amended, if appropriate)
4. ☒ Drawing(s) (proposed amendments, if appropriate)
   - ☒ Transfer drawings from original patent file
5. ☒ Reissue Oath/Declaration (original or copy) (37 C.F.R. § 1.175) (PTO/SB/51 or 52)
6. Original U.S. Patent currently assigned
   - ☒ Yes ☐ No
   - ☒ Written Consent of all Assignees (PTO/SB/53)
   - ☒ 37 C.F.R. § 3.73(b) Statement (PTO/SB/96)
   - ☒ Power of Attorney

ACCOMPANYING APPLICATION PARTS

7. ☒ Statement of Status/Support for all changes to the claims embedded in the remarks of the preliminary amendment. See 37 CFR 1.173(c).
8. ☐ Original U.S. Patent for Surrender
   - ☐ Ribboned Original Patent Grant
   - ☐ Statement of Loss (PTO/SB/55)
9. ☐ Foreign Priority Claim (35 U.S.C. 119) if applicable
10. ☒ Information Disclosure Statement (IDS)/PTO-1449
    - ☒ Copies of IDS Citations
11. ☐ English Translation of Reissue Oath/Declaration
12. ☒ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503)
14. ☒ Other: <u>Petition for Waiver under 1.183</u>

15. CORRESPONDENCE ADDRESS

☒ Customer Number 25696 or ☒ Correspondence address below

Name	Oppenheimer Wolff & Donnelly LLP				
Address	1400 Page Mill Rd.				
City	Palo Alto	**State**	California	**Zip Code**	94303
Country	USA	**Telephone**	(650) 320-4000	**Fax**	(650) 320-4100
Name	LEAH SHERRY	**Registration No.**	43,918		
Signature		**Date**	10/20/00		

SV/108804.01
10142000/10.40/20206.14

PTO/SB/56 (08-00)
Approved for use through 12/30/2000. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REISSUE APPLICATION FEE TRANSMITTAL FORM

Docket Number: 20206-014(PT-TA-410)
Patent: 5,848,159

Claims as Filed – Part 1

Claims in Patent		Number filed in Reissue Application	(3) Number Extra	Small Entity		Other than Small Entity	
				Rate	Fee	Rate	Fee
(A) 13	Total Claims (37 CFR 1.16(j))	(B) 61	= 48	x$_____		x$18.00	$864.00
(C) 8	Independent Claims (37CFR 1.16(i))	(D) 20	= 12	x$_____		x$80.00	$960.00
Basic Fee (37 CFR 1.16(h)) $710.00						OR	$_____
Total Filing Fee $2,534.00							$_____

Claims as Amended – Part 2

	(1) Claims Remaining After Amendment		(2) Highest Number Previously Paid For	(3) Extra Claims Present	Small Entity		Other than a Small Entity	
					Rate	Fee	Rate	Fee
Total Claims (37 CFR 1.16(j))	13	MINUS	20	*= 0	x$_____=		x$ 0 =	
Independent Claims (37 CFR 1.16(i))	8	MINUS	8	= 0	x$_____=		x$ 0 =	
Total Additional Fee						$0	OR	$

* if the entry in (D) is less than the entry in (C), Write "0" in column 3.

** If the "Highest Number of Total Claims Previously Paid For" is less than 20, write "20" in this space.

*** After any cancellation of claims.

**** If "A" is greater than 20, use (B-A); if "A" is 20 or less, use (B-20).

***** Highest Number of Independent Claims Previously Paid For" or Number of Independent Claims in Patent (C).

□ Applicant claims small entity status. See 37 CFR 1.27.

□ Please charge Deposit Account No. 02-3964 in the amount of $________________________.

A duplicate copy of this sheet is enclosed for this purpose.

☒ The Commissioner if hereby authorized to charge any additional fees under 37 CFR 1.16 or 1.17 which may be required, or credit any overpayments to Deposit Account No. 02-3964.

A duplicate copy of this sheet is enclosed for this purpose.

☒ A check in the amount of $2,664.00, to cover the filing fee and petition fee under 1.17(h), is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038

10/20/00
Date

Leah Sherry, Registration No. 43,918
Attorney for Patentee

IN THE UNITED STATES PATENTS AND TRADEMARK OFFICE

Applicant: COLLINS et al. Attorney Docket No.: 20206-0014(PT-TA-410)

Patent No.: **5,848,159**

Issued: December 8, 1998

For: **"PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD"**

CERTIFICATE UNDER 37 CFR 3.73(b)

I. Compaq Computer Corporation, a Delaware corporation, certifies that it is the assignee of the entire right, title, and interest in the patent application identified above by virtue of a chain of title from the inventors of the patent application identified above, to the current assignee as shown below:

1. From: Thomas Collins, Dale Hopkins, Susan Langford and Michael Sabin
   To: Tandem Computers Incorporated

   The document was recorded in the Patent and Trademark Office on May 7, 1997 as Reel and Frame # 8542/0875.

2. From: Tandem Computers Incorporated
   To: Compaq Computer Corporation

   The document was recorded in the Patent and Trademark Office on October 12, 2000, a copy of which is attached.

II. The undersigned is empowered to sign this certificate on behalf of the assignee.

Date: 14 OCT 00

Theodore S. Park
Senior Counsel, Intellectual Property

Compaq Computer Corporation
P.O. Box 692000
Houston, TX 7707-2698

REISSUE APPLICATION BY THE INVENTOR(S), OFFER TO SURRENDER PATENT	Docket Number: 20206-014(PT-TA-410) Patent: 5,848,159

This is part of the application for a reissue patent based on the original patent identified below.

Name of Patentee(s)	Thomas Collins, Dale Hopkins, Susan Langford, Micahel Sabin		
Patent Number	5,848,159	Date Patent Issued	December 8, 1998
Title of Invention	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD		

I am the

□ inventor (if only one name is listed herein) of the original patent.

☒ joint inventor (if plural names are listed herein) of the original patent.

I offer to surrender the original patent.

1. ☒ Filed herein is a certificate under 37 CFR 3.73(b).

2. □ Ownership of the patent is in the inventor(s), and no assignment of the patent has been made.

One of boxes 1 or 2 above must be checked.

The written consent of all assignees owning an undivided interest in the original patent is included in this application for reissue.

Signature		Date:	
Typed or printed name:	Thomas Collins		
Signature		Date:	
Typed or printed name:	Dale Hopkins		
Signature		Date:	
Typed or printed name:	Susan Langford		
Signature		Date:	
Typed or printed name:	Michael Sabin		

The assignee owning an undivided interest in said original patent is Compaq Computer Corporation, and the assignee consents to the accompanying application for reissue.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that suck willful false statements may jeopardize the validity of the application, any patent issued thereon, or any patent to which this declaration is directed.

Name of Assignee	Compaq Computer Corporation
Signature of Person Signing for the Assignee	
Type/printed name and title of person signing for assignee	Theodore S. Park, Senior Intellectual Property Counsel

CONSENT OF ASSIGNEE TO REISSUE APPLICATION	Docket Number: 20206-014(PT-TA-410)

This is part of the application for a reissue patent based on the original patent identified below.

Name of Patentee(s):	COLLINS et al.		
Patent Number:	5,848,159	Patent Issued	December 8, 1998
Title of Invention	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD		

As an authorized agent empowered to act on behalf of Compaq Computer Corporation, the assignee of the entire interest in the original patent, I hereby consent to the filing of the present application for reissue of the original patent.

☒ A certificate under 37 CFR(b) is attached.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application, any patent issued thereon, or any patent to which this declaration is directed.

Name of Assignee	Compaq Computer Corporation
Signature of Person Signing for Assignee	
Printed name and title of person signing for assignee	Theodore S. Park, Counsel

PTO/SB/53 (12-97)
Approved for use through 9/30/00. OMB 0651-0033
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REISSUE APPLICATION BY THE INVENTOR(S), OFFER TO SURRENDER PATENT	Docket Number: 20206-014(PT-TA-410) Patent: 5,848,159

This is part of the application for a reissue patent based on the original patent identified below.

Name of Patentee(s)	Thomas Collins, Dale Hopkins, Susan Langford, Michael Sabin		
Patent Number	5,848,159	Date Patent Issued	December 8, 1998
Title of Invention	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD		

I am the

□ inventor (if only one name is listed herein) of the original patent.

☒ joint inventor (if plural names are listed herein) of the original patent.

I offer to surrender the original patent.

1. ☒ Filed herein is a certificate under 37 CFR 3.73(b).

2. □ Ownership of the patent is in the inventor(s), and no assignment of the patent has been made.

One of boxes 1 or 2 above must be checked.

The written consent of all assignees owning an undivided interest in the original patent is included in this application for reissue.

Signature	Thomas Collins	Date:	Oct. 20, 2000
Typed or printed name:	Thomas Collins		
Signature	Dale Hopkins	Date:	Oct. 20, 2000
Typed or printed name:	Dale Hopkins		
Signature	Susan K Langford	Date:	Oct. 20, 2000
Typed or printed name:	Susan Langford		
Signature		Date:	
Typed or printed name:	Michael Sabin		

The assignee owning an undivided interest in said original patent is Compaq Computer Corporation, and the assignee consents to the accompanying application for reissue.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that suck willful false statements may jeopardize the validity of the application, any patent issued thereon, or any patent to which this declaration is directed.

Name of Assignee	Compaq Computer Corporation
Signature of Person Signing for the Assignee	
Type/printed name and title of person signing for assignee	Theodore S. Park, Senior Intellectual Property Counsel

PTO/SB/53 (12-97)
Approved for use through 9/30/00. OMB 0651-0033
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REISSUE APPLICATION BY THE INVENTOR(S), OFFER TO SURRENDER PATENT	Docket Number: 20206-014(PT-TA-410) Patent: 5,848,159

This is part of the application for a reissue patent based on the original patent identified below.

Name of Patentee(s)	Thomas Collins, Dale Hopkins, Susan Langford, Michael Sabin		
Patent Number	5,848,159	Date Patent Issued	December 8, 1998
Title of Invention	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD		

I am the

☐ inventor (if only one name is listed herein) of the original patent.

☒ joint inventor (if plural names are listed herein) of the original patent.

I offer to surrender the original patent.

1. ☒ Filed herein is a certificate under 37 CFR 3.73(b).

2. ☐ Ownership of the patent is in the inventor(s), and no assignment of the patent has been made.

One of boxes 1 or 2 above must be checked.

The written consent of all assignees owning an undivided interest in the original patent is included in this application for reissue.

Signature		Date:	
Typed or printed name:	Thomas Collins		
Signature		Date:	
Typed or printed name:	Dale Hopkins		
Signature		Date:	
Typed or printed name:	Susan Langford		
Signature	Mull J. Sabin	Date:	20 OCT 2000
Typed or printed name:	Michael Sabin		

The assignee owning an undivided interest in said original patent is Compaq Computer Corporation, and the assignee consents to the accompanying application for reissue.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that suck willful false statements may jeopardize the validity of the application, any patent issued thereon, or any patent to which this declaration is directed.

Name of Assignee	Compaq Computer Corporation
Signature of Person Signing for the Assignee	
Type/printed name and title of person signing for assignee	Theodore S. Park, Senior Intellectual Property Counsel

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Attorney Docket No. 20206-014(PT-TA-410)

Inventors: Collins et al.

Patent No. **5,848,159**

Issued: December 8, 1998

For: **PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD**

CERTIFICATE OF MAILING
I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service as Express Mail No. EL655031318US addressed to: Assistant Commissioner for Patents, Box: DAC, Washington, DC, 20231 on October 19, 2000,

By:

Assistant Commissioner for Patents
Box: Reissue
Washington, D.C. 20231

REISSUE APPLICATION PRELIMINARY AMENDMENT

Sir:

In conjunction with the filing of a Reissue Application, please amend the specification of the above-mentioned U.S. Patent and consider the remarks as hereafter provided:

In the Specification other than Claims:

Replace the paragraph beginning at column (hereafter "col.") 1, line 4 with the following:

This application claims the benefit of U.S. Provisional Application No. 60/033,271 for PUBLIC KEY CRYTOGRAPHIC APPARATUS AND METHOD, filed Dec. 9, 1996, naming as inventors, Thomas [Colins] Collins, Dale Hopkins, Susan Langford and [Michale] Michael Sabin, the [discolsure] disclosure of which is incorporated by reference.

Replace the paragraph beginning at col. 1, line 64 with the following:

The RSA scheme capitalizes on the relative ease of creating a composite number from the product of two prime numbers whereas the attempt to factor the composite number into its constituent primes is difficult. The RSA scheme uses a public key E comprising a pair of positive integers n and e, where n is a composite number of the form

$$n=p\cdot q \qquad (1)$$

where p and q are different prime numbers, and e is a number relatively prime to (p-1) and (q-1); that is, e is relatively prime to (p-1) or (q-1) if e has no factors in common with either of them. Importantly, the sender has access to n and e, but not to p and q. The message M is a number representative of a message to be transmitted wherein

$$0\leq M\leq n\text{-}1. \qquad (2)$$

The sender enciphers M to create ciphertext C by computing the exponential

$$[C=M^e(\mathrm{mod}\ n)]\ \underline{C\equiv M^e(\mathrm{mod}\ n)}. \qquad (3)$$

Replace the paragraph beginning at col. 2, line 19 with the following:

The recipient of the ciphertext C retrieves the message M using a (private) decoding key D, comprising a pair of positive integers d and n, employing the relation

$$[M=C^d\ (\mathrm{mod}\ n)]\ \underline{C\equiv M^d(\mathrm{mod}\ n)} \qquad (4)$$

As used in (4), above, d is a multiplicative inverse of

$$e(\mathrm{mod}(\mathrm{lcm}((p\text{-}1),(q\text{-}1)))) \qquad (5)$$

so that

$$[e\cdot d=1(\mathrm{mod}(\mathrm{lcm}((p\text{-}1),(q\text{-}1))))]\ \underline{e\cdot d\equiv 1(\mathrm{mod}(\mathrm{lcm}((p\text{-}1),(q\text{-}1))))} \qquad (6)$$

where lcm((p-1), (q-1)) is the least common multiple of numbers p-1 and q-1. Most commercial implementations of RSA employ a different, although equivalent, relationship for obtaining d:

$$[d=e^{-1}\ \mathrm{mod}(p\text{-}1)\ (q\text{-}1)]\ \underline{d\equiv e^{-1}\ \mathrm{mod}((p\text{-}1)\cdot(q\text{-}1))}. \qquad (7)$$

This alternate relationship simplifies computer processing.

Replace the paragraph beginning at col. 3, line 23 with the following:

It is still another object of this invention to provide a system and method for implementing an RSA scheme in which the [components] factors of n do not increase in length as n increases in length.

Replace the paragraph beginning at col. 3, line 27 with the following:

It is still another object to provide a system and method for utilizing multiple (more than two), distinct prime number [components] factors to create n.

Replace the paragraph beginning at col. 3, line 36 with the following:

The present invention discloses a method and apparatus for increasing the computational speed of RSA and related public key schemes by focusing on a neglected area of computation inefficiency. Instead of $n=p\cdot q$, as is universal in the prior art, the present invention discloses a method and apparatus wherein n is developed from three or more distinct random prime numbers; i.e., $n=p_1\cdot p_2 \cdot. . .\cdot p_k$, where k is an integer greater than 2 and p_1, p_2,. . . p_k are sufficiently large distinct random primes. Preferably, "sufficiently large primes" are prime numbers that are numbers approximately 150 digits long or larger. The advantages of the invention over the prior art should be immediately apparent to those skilled in this art. If, as in the prior art, p and q are each on the order of, say, 150 digits long, then n will be on the order of 300 digits long. However, three primes p_1, p_2 and p_3 employed in accordance with the present invention can each be on the order of 100 digits long and still result in n being 300 digits long. Finding and verifying 3 distinct primes, each 100 digits long, requires significantly fewer computational cycles than finding and verifying 2 primes each 150 digits long.

Replace the paragraph beginning at col. 3, line 56 with the following:

The commercial need for longer and longer primes shows no evidence of slowing; already there are projected requirements for n of about 600 digits long to forestall incremental improvements in factoring techniques and the ever faster computers available to break ciphertext. The invention, allowing 4 primes each about 150 digits long to obtain a 600 digit n, instead of two primes about [350] 300 digits long, results in a marked improvement in computer performance. For, not only are primes that are 150 digits in size easier to find and verify than ones on the order of [350] 300 digits, but by applying techniques the inventors derive from the Chinese Remainder Theorem (CRT), public key cryptography calculations for encryption and decryption are completed much faster--even if performed serially on a single processor system. However, the inventors' techniques are particularly adapted to [be] advantageously apply [enable] RSA public key cryptographic operations to parallel computer processing.

Replace the paragraph beginning at col. 4, line 6 with the following:

The present invention is capable of [using] extending the RSA scheme to perform encryption and decryption operation using a large (many digit) n much faster than heretofore possible. Other advantages of the invention include its employment for decryption without the need to revise the RSA public key encryption transformation scheme currently in use on thousands of large and small computers.

Replace the paragraph beginning at col. 4, line 13 with the following:

A key assumption of the present invention is that n, composed of 3 or more sufficiently large distinct prime numbers, is no easier (or not very much easier) to factor than the prior art, two prime number n. The assumption is based on the observation that there is no indication in the prior art literature that it is "easy" to factor a product consisting of more than two sufficiently large, distinct prime numbers. This assumption may be justified given the continued effort (and failure) among experts to find a way "easily" to break large [component] composite numbers into their large prime factors. This assumption is similar, in the inventors' view, to the assumption underlying the entire field of public key cryptography that factoring composite numbers made up of two distinct primes is not "easy." That is, the entire field of public key cryptography is based not on mathematical proof, but on the assumption that the empirical evidence of failed sustained efforts to find a way systematically to solve NP problems in polynomial time indicates that these problems truly are "difficult."

Replace the paragraph beginning at col. 4, line 32 with the following:

The invention is preferably implemented in a system that employs parallel operations to perform the encryption, decryption operations required by the RSA scheme. Thus, there is also disclosed a cryptosystem that includes a central processor unit (CPU) coupled to a number of exponentiator elements. The exponentiator elements are special purpose arithmetic units designed and structured to be provided message data M, an encryption key e, and a number n (where [$n=p_1 * p_2 * \ldots p_k$] $\underline{n= p_1 \cdot p_2 \cdot \ldots \cdot p_k}$, k being greater than 2) and return ciphertext C according to the relationship,

$$[C=M^e \ (\mathrm{mod}(n))] \ \underline{C \equiv M^e \ (\mathrm{mod}\ n)}.$$

Replace the paragraph beginning at col. 4, line 45 with the following:

Alternatively, the exponentiator elements may be provided the ciphertext C, a decryption (private) key d and n to return M according to the relationship,

$$[M=C^d \ (\mathrm{mod}(n))] \ \underline{M \equiv C^d \ (\mathrm{mod}\ n)}$$

Replace the paragraph beginning at col. 4, line 50 with the following:

According to this decryption aspect of the invention, the CPU receives a task, such as the requirement to decrypt [cyphertext] ciphertext data C. The CPU will also be provided, or have available, a [public] private key [e] d and n, and the factors of n (p_1, p_2, . . . p_k). The CPU breaks the [encryption] decryption task down into a number of sub-tasks, and delivers the sub-tasks to the exponentiator elements. [When the] The results of the sub-tasks are returned by the exponentiator elements to the CPU which [will], using a form of the CRT, combines the results to obtain the message data M. An encryption task may be performed essentially in the same manner by the CPU and its use of the exponentiator elements. However, usually the factors of n are not available to the sender (encryptor), only the public key, e and n, so that no sub-tasks are created.

Before the paragraph beginning at col. 5, line 52, ***insert*** *the following paragraph:*

Alternatively, a message data M can be encoded with the private key to a signed message data M_S using a relationship of the form

$$M_s \equiv M^d (\bmod n).$$

The message data M can be reproduce from the signed message data M_S by decoding the signed data with the public key, using a relationship of the form

$$M \equiv M_s^e (\bmod n).$$

Replace the paragraph beginning at col. 5, line 30 with the following:

According to the present invention, the public key portion e is picked. Then, three or more random large, distinct prime numbers, p_1, p_2, . . . , p_k are developed and checked to ensure that each (p_i-1) is relatively prime to e. Preferably, the prime numbers are of equal length. Then, the product [n=p_1, p_2, . . . , p_k] $n = p_1 \cdot p_2 \cdot \ldots p_k$ is computed.

Replace the paragraph beginning at col. 5, line 36 with the following:

Finally, the decryption [key] exponent, d, is established by the relationship:

[$d=e^{-1}$ mod ((p_1 -1) (p_2 -1) . . . (p_k -1))] $d\equiv e^{-1}$ mod ((p_1 -1)·(p_2 -1)· . . .·(p_k - 1)), or equivalently

$d\equiv e^{-1}$ mod (lcm((p_1 -1), (p_2 -1), . . . (p_k -1)))

Replace the paragraph beginning at col. 5, line 41 with the following:

The message data, M is encrypted to ciphertext C using the relationship of (3), above, i.e.,

$$[C=M^e \bmod n.]\ \underline{C\equiv M^e \pmod{n}}$$

Replace the paragraph beginning at col. 5, line 46 with the following:

To decrypt the ciphertext, C, the relationship of [(3)] $\underline{(4)}$, above, is used:

$$[M=C^d \bmod n]\ \underline{M\equiv C^d \pmod{n}}$$

where n and d are those values identified above.

Replace the paragraph beginning at col. 5, line 52 with the following:

Using the present invention involving three primes to develop the product n, RSA encryption and decryption time can be substantially less than an RSA scheme using two primes by dividing the encryption or decryption task into sub-tasks, one sub-task for each distinct prime. (However, breaking the encryption or decryption into subtasks requires knowledge of the factors of n. This knowledge is not usually available to anyone except the owner of the key, so the encryption process can be accelerated only in special cases, such as encryption for local storage. A system encrypting data for another user performs the encryption process according to (3), independent of the number of factors of n. Decryption, on the other hand, is performed by the owner of a key, so the factors of n are generally known and can be used to accelerate the process.) For example, assume that three distinct primes, p_1, p_2, and p_3, are used to develop the product n. Thus, decryption of the ciphertext, C, using the relationship

$$[M=C^d (\bmod n)]\ \underline{M\equiv C^d (\bmod n)}$$

is used to develop the decryption sub-tasks:

$$[M_1 = C_1^{d_1} \bmod p_1]\ \underline{M_1 \equiv C_1^{d_1} (\bmod p_1)}$$

$$[M_2 = C_2^{d_2} \bmod p_2]\ \underline{M_2 \equiv C_2^{d_2} (\bmod p_2)}$$

$$[M_3 = C_3^{d_3} \bmod p_3]\ \underline{M_3 \equiv C_3^{d_3} (\bmod p_3)}$$

where

$$[C_1 = C \bmod p_1;]\ \underline{C_1 \equiv C\ (\bmod\ p_1)};$$

$$[C_2 = C \bmod p_2;]\ \underline{C_2 \equiv C\ (\bmod\ p_2)};$$

$$[C_3 = C \bmod p_3\ ;]\ \underline{C_3 \equiv \mathrm{C}\ (\bmod\ p_3)};$$

$$[d_1 = d \bmod (p_1 - 1)]\ \underline{d_1 \equiv d\ (\bmod\ (p_1 - 1))};$$

$$[d_2 = d \bmod (p_2 - 1)]\ \underline{d_2 \equiv d\ (\bmod\ (p_2 - 1))};\ \text{and}$$

$$[d_3 = d \bmod (p_3 - 1)]\ \underline{d_3 \equiv d\ (\bmod\ (p_3 - 1))}.$$

Replace the paragraph beginning at col. 6, line 24 with the following:

The results of each sub-task, M_1, M_2, and M_3 can be combined to produce the plaintext, M, by a number of techniques. However, it is found that they can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using, preferably, a recursive scheme. Generally, the plaintext M is obtained from the combination of the individual sub-tasks by the following relationship:

$$\underline{Y_i \equiv Y_{i-1} + ((M_i - Y_{i-1})\ (w_i^{-1}\ (\bmod\ p_i))\ (\bmod\ p_i)) \cdot w_i\ (\bmod\ n)}\ [Y_i = Y_{i-1} + [(M_i - Y_{i-1})\ (w_i^{-1} \bmod p_i) \bmod p_i] \cdot w_i \bmod n]$$

where [i ≥2] $\underline{2 \le i \le k \text{ where k is the number of prime factors of n,}}$ and

$$M = Y_k,\ Y_1 = C_1,\ and\ w_i = \prod_{j<i} p_j$$

Encryption is performed in much the same manner as that used to obtain the plaintext M, provided (as noted above) the factors of n are available. Thus, the relationship

$$[C = M^e\ (\bmod\ n)]\ \underline{C \equiv M^e\ (\bmod\ n)},$$

can be broken down into the three sub-tasks,

$$[C_1 = M_1^{e1} \bmod p_1]\ \underline{C_1 = M_1^{e_1} (\bmod p_1)},$$

[$C_2 = M_2^{e2} \bmod p_2$] $C_2 = M_2^{e_2} (\bmod p_2)$ and

[$C_3 = M_3^{e3} \bmod p_3$] $C_3 = M_3^{e_3} (\bmod p_3)$,

where

[$M_1 = M(\bmod p_1)$] $M_1 \equiv M (\bmod p_1)$,

[$M_2 = M(\bmod p_2)$] $M_2 \equiv M (\bmod p_2)$,

[$M_3 = M(\bmod p_3)$] $M_3 \equiv M (\bmod p_3)$,

[$e_1 =$emod $(p_1 - 1)$] $e_1 \equiv e \bmod (p_1 - 1)$,

[$e_2 =$emod $(p_2 - 1)$] $e_2 \equiv e \bmod (p_2 - 1)$, and

[$e_3 =$emod $(p_3 - 1)$] $e_3 \equiv e \bmod (p_3 - 1)$.

Replace the paragraph beginning at col. 6, line 65 with the following:

In generalized form, the ciphertext C (i.e., [decrypted] encrypted message M) can be obtained by [the same summation] a recursive scheme as identified above to obtain the ciphertext C from its contiguous constituent sub-tasks C_i.

Replace the paragraph beginning at col. 7, line 1 with the following:

Preferably, the recursive CRT method described above is used to obtain either the ciphertext[,] C[,] or the deciphered plaintext (message) M due to its speed. However, there may be [occasions] implementations when it is beneficial to use a non-recursive technique in which case the following relationships are used:

$M \equiv \sum_{i=1}^{k} M_i (w_i^{-1} (\bmod p_i)) \cdot w_i (\bmod n)$ [$M = \sum_{i=1}^{k} M_i (w_i^{-1} \bmod p_i)\, w_i \bmod$ n]

where

$$[w_i = \prod_{j \neq 1} p_j]\ \underline{w_i = \prod_{j \neq i} p_j}, \text{ and}$$

k is the number (3 or more) of distinct primes chosen to develop the product n.

Replace the paragraph beginning at col. 7, line 17 with the following:

Thus, for example above (k=3), M is constructed from the returned sub-task values M_1, M_2, M_3 by the relationship

$$[M{=}M_1\,(w_1^{-1} \bmod p_1)\, w_1 \bmod/n{+}M_2\,(w_2^{-1} \bmod p_2)\, w_2 \bmod n +$$

$$M_3\,(w_3^{-1} \bmod p_3)\, w_3 \bmod n]\ \underline{M \equiv M_1\,(w_1^{-1}\,(\text{mod}\,p_1))\cdot w_1\,(\text{mod}\,n)}$$

$$\underline{+\,M_2\,(w_2^{-1}\,(\text{mod}\,p_2))\cdot w_2\,(\text{mod}\,n)}$$

$$\underline{+\,M_3\,(w_3^{-1}\,(\text{mod}\,p_3))\cdot w_3\,(\text{mod}\,n)}$$

where

$$w_1 = p_2\,p_3,\ w_2 = p_1\,p_3, \text{ and } w_3 = p_1\,p_2.$$

Replace the paragraph beginning at col. 7, line 52 with the following:

The I/O bus 30 communicatively connects the CPU to a number of exponentiator elements [32_a, 32_b, and 32_c]32a, 32b and 32c. Shown here are three exponentiator elements, although as illustrated by the "other" exponentiators [32_n]32n, additional exponentiator elements can be added. Each exponentiator element is a state machine controlled arithmetic circuit structured specifically to implement the relationship described above. Thus, for example, the exponentiator 32a would be provided the values M_1, e_1, and p_1[, n] to develop C_1. Similarly, the exponentiator circuits 32b and 32c develop C_2 and C_3 from corresponding subtask values M_2, e_2, [P_2]p_2, M_3, e_3, and [P_3]p_3.

Replace the paragraph beginning at col. 8, line 1 with the following:

In order to ensure a secure environment, it is preferable that the cryptosystem 10 meet the Federal Information [Protection System] Processing Standard (FIPS) 140-1 level 3. Accordingly, the elements that make up the CPU 14 would be implemented in a design that will be secure from external probing of the circuit. However, information communicated on the I/O bus 30 between the CPU 14 and the exponentiator circuits 32 (and external memory 34--if present) is exposed. Consequently, to maintain the security of that information, it is first encrypted by the DES unit 24 before it is placed on the I/O bus 30 by the CPU 14. The exponentiator circuits 32, as well as the external memory 34, will also include similar DES units to decrypt information received from the CPU, and later to encrypt information returned to the CPU 14.

Replace the paragraph beginning at col. 8, line 52 with the following:

In similar fashion, information is conveyed to or retrieved from the exponentiators 32 by the processor 20 by write or read operations at addresses within the address range 44. Consequently, writes to the exponentiators 32 will use the DES unit 24 to encrypt the information. When that (encrypted) information is received by the exponentiators 32, it is decrypted by on-board DES units (of each exponentiator 32). The result[s] of the task performed by the exponentiator 32 is then encrypted by the exponentiator's on-board DES unit, retrieved by the processor 20 in encrypted form and then decrypted by the DES unit 24.

Replace the paragraph beginning at col. 9, line 24 with the following:

Assume, for the purpose of the remainder of this discussion, that the encryption/decryption tasks performed by the cryptosystem 10, using the present invention, employs only three distinct primes, p_1, p_2, p_3. The processor 20 will develop the sub tasks identified above, using M, e, p_1 p_2, p_3 Thus, for example, if the exponentiator 32a were assigned the sub-task of developing C_1, the processor would develop the values M_1[,] and e_1[, and (p_1 -1)] and deliver [units] (write) these values, with

[n]p_1, to the exponentiator 32a. Similar values will be developed by the processor 20 for the sub-tasks that will be delivered to the exponentiators 32b and 32c.

Replace the paragraph beginning at col. 10, line 15 with the following:

Alternatively, the [post]host-system 50 may desire to deliver, via the communication medium 60, an encrypted communication to one of the stations 64. If the communication is to be encrypted by the DES scheme, with the DES key encrypted by the RSA scheme, the host system would encrypt the communication, forward the DES key to one of the cryptosystems 10 for encryption via the RSA scheme. When the encrypted DES key is received back from the cryptosystem 10, the host system can then deliver to one or more of the stations 64 the encrypted message.

Replace the paragraph beginning at col. 10, line 25 with the following:

Of course, the host system 50 and the stations 64 will be using the RSA scheme of public key encryption/decryption. Encrypted communications from the stations 64 to the host system 50 require that the stations 64 have access to the public key [E (E, N)] E=(e, n) while the host system maintains the private key [D (D, N,] D=(d, n) and the constituent primes, $p_1, p_2, \ldots, p_k$). Conversely, for secure communication from the host system 50 to one or more of the stations 64, the host system would retain a public key E' for each station 64, while the stations retain the corresponding private keys [E'] D'.

Replace the paragraph beginning at col. 10, line 35 with the following:

Other techniques for encrypting the communication could used. For example, the communication could be entirely encrypted by the RSA scheme. If, however, the message to be communicated[ion] is represented by a numerical value greater than n-1, it will need to be broken up into blocks size M where

$$[0 \leq M \leq N-1]\ 0 \leq M \leq n\text{-}1.$$

In the Claims

Amend claims 1-13 (following the format of the claims as presented herein, including insertion of new lines and indentations where applicable), and add new claims 14-61 as follows:

1. (Amended) A method [for establishing] of processing a message for use in cryptographic communications comprising the steps of:

developing a composite number, n, as a product of $p_1 \cdot p_2 \cdot . . . . \cdot p_k$ where k is an integer greater than 2, and p_1, p_2, . . . p_k are distinct random prime numbers; and

encoding a plaintext message word signal M to a ciphertext word signal C, where M corresponds to a number representative of [a] the message and

$0 \leq M \leq n-1$,

[n being a composite number formed from the product of $p_1 \cdot p_2 \cdot . . . . \cdot p_k$ where k is an integer greater than 2, p_1, p_2, . . . p_k are distinct prime numbers, and] where C is a number representative of an encoded form of the plaintext message word signal M such that

$C \equiv M^e \pmod{n}$, and [, wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby

$C=M^e \pmod{n}$]

where e is a number relatively prime to $(p_1 - 1) \cdot (p_2 - 1) \cdot . . . \cdot (p_k - 1)$.

2. (Amended) The method according to claim 1, comprising the further step of:

establishing a number, d, as a multiplicative inverse of

$e(\bmod(\operatorname{lcm}((p_1 -1), (p_2 -1), ... , (p_k -1))))$; and

decoding the ciphertext word signal C to the plaintext message word signal M[, wherein said decoding step comprises the step of: transforming said ciphertext word signal C] where[by:]

$[M=C^d \pmod{n}]$ $M \equiv C^d \pmod{n}$

[where d is a multiplicative inverse of e(mod(lcm((p_1 -1), (p_2 -1), . . . , (p_k -1))))].

3. (Amended) A method [for transferring] of processing a message signal M_i for use in a communications system having j terminals, [wherein] each terminal [is] being characterized by an encoding key $E_i =(e_i, n_i)$ and decoding key $D_i =(d_i, n_i)$, where i=1, 2, . . . , j, and [wherein] the message signal M_i [corresponds] corresponding to a number representative of a message-to-be-transmitted from the i^th terminal, the method comprising the steps of:

computing n_i where n_i is a composite number of the form

[$n_i =P_{i,1} \cdot p_{i,2} \cdot, . . . ,\cdot p_{i,k}$] $n_i = p_{i,1} \cdot p_{i,2} \cdot, . . . ,\cdot p_{i,k}$

where k is an integer greater than 2,

$p_{i,1}, p_{i,2}, . . . , p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to [lcm($p_{i,1}$ -1, $p_{1,2}$ -1, $p_{i,k}$ -1)] lcm($p_{i,1}$ -1, $p_{i,2}$ -1,... $p_{i,k}$ -1), and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_i (mod(lcm(($p_{i,1}$ -1), ($p_{i,2}$ -1), . . . , ($p_{i,k}$ -1))));[,

comprising the step of:]

encoding a digital message word signal [M_A]M_1 for transmission from a first terminal (i=1[A]) to a second terminal (i=2[B]), said encoding step including the sub-step of:

transforming said message word signal [M_A]M_1 to one or more message block word signals [M_A"]M_1", each block word signal [M_A"]M_1" corresponding to a number representative of a portion of said message word signal [M_A]M_1 in the range $0\leq M_A" \leq n_2-1$ [$0\leq M_A" \leq n_B -1$],

transforming each of said message block word signals [M_A"]M_1" to a ciphertext word signal [C_A, C_A corresponding] C_1 that corresponds to a number representative of an encoded form of said message block word signal [M_A"]M_1"[,] where[by:]

[$C_A \equiv M_A{}^{"eB} \pmod{n_B}$] $C \equiv M_1{}^{"e_1} \pmod{n_2}$.

4. (Amended) A cryptographic communications system comprising:

a communication [medium] channel adapted for transmitting a ciphertext word signal C that relates to a transmit message word signal M;

[an]encoding means coupled to said channel and adapted for transforming [a] the transmit message word signal M to [a] the ciphertext word signal C using a composite number, n, where n is a product of the form

$n= p_1 \cdot p_2 \cdot \ldots \cdot p_k$

k is an integer greater than 2, and

$p_1, p_2, \ldots p_k$ are distinct random prime numbers [and for transmitting C on said channel],

where the transmit message word signal M corresponds to a number representative of a message and

$0 \leq M \leq n-1$ [where n is a composite number of the form

$n=p_1 \cdot p_2 \cdot \ldots \cdot p_k$

where k is an integer greater than 2 and $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and]

where the ciphertext word signal C corresponds to a number representative of an [enciphered] encoded form of said message through a relationship of the form[and corresponds to]

$C \equiv M^e \pmod{n}$, and

where e is a number relatively prime to lcm(p1 -1, p2 -1, . . . , pk -1); and

[a]decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and for transforming the ciphertext word signal C to a receive message word signal M' where M' corresponds to a number representative of a [deciphered] decoded form of the ciphertext word signal C [and corresponds to] through a relationship of the form

$M' \equiv C^d \pmod{n}$

where d is selected from the group consisting of [the] a class of numbers equivalent to a multiplicative inverse of

$e(\mathrm{mod}(\mathrm{lcm}((p_1 -1), (p_2 -1), \ldots, (p_k -1))))$.

5. (Amended) A cryptographic communications system having a plurality of terminals coupled by a communications channel, [including] comprising:

a first terminal of the plurality of terminals characterized by an [associated] encoding key $E_A = (e_A, n_A)$ and a decoding key $D_A = (d_A, n_A)$,

where[in] n_A is a composite number of the form

$n_A = p_{A,1} \cdot p_{A,2} \cdot \ldots \cdot p_{A,k}$

where

k is an integer greater than 2,

$p_{A,1}, p_{A,2}, \ldots, p_{A,k}$ are distinct random prime numbers,

e_A is relatively prime to

$\mathrm{lcm}(p_{A,1} -1, p_{A,2} -1, \ldots, p_{A,k} -1)$, and

d_A is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_A (\mathrm{mod}(\mathrm{lcm}((p_{A,1} -1), (p_{A,2} -1), \ldots, (p_{A,k} -1))))$; and[,]

[and including]a second terminal of the plurality of terminals having[, comprising:]

blocking means for transforming a first message, [-to-be-transmitted] which is to be transmitted on said communications channel from said second terminal to said first terminal, to one or more transmit message word signals M_B, where each M_B corresponds to a number representative of said message in the range

$0 \leq M_B \leq n_A -1$,

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that [and for transmitting

C_B on said channel, where C_B] corresponds to a number representative of an [enciphered] encoded form of said first message [and corresponds to] through a relationship of the form

$$[C_B \equiv M_B^{eA} (\text{mod } n_A)] \; \underline{C_B \equiv M_B{}^{e_A} (\text{mod}\, n_A)},$$

[wherein]said first terminal having [comprises:]

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_B from said channel and for transforming each of said ciphertext word signals $\underline{C_B}$ to a receive message word signal [M_B]$\underline{M'_B}$, and

means for transforming said receive message word signal[s] [M']$\underline{M'_B}$ to said first message, where [M']$\underline{M'_B}$ [is] corresponds to a number representative of a [deciphered] decoded form of C_B [and corresponds to] through a relationship of the form

$$[M_B' \equiv C_B^{da} (\text{mod } n_A)] \; \underline{M'_B \equiv C_B{}^{d_A} (\text{mod}\, n_A)}.$$

6. (Amended) The system according to claim 5 wherein said second terminal is characterized by an [associated] encoding key [$E_B = (e_B, n_B)$]$\underline{E_B = (e_B, n_B)}$ and a decoding key [$DB = (D_B, d_B)$]$\underline{D_B = (d_B, n_B)}$, where[:

] n_B is a composite number of the form

$$n_B = p_{B,1} \cdot p_{B,2} \cdot \ldots \cdot p_{B,k}$$

where k is an integer greater than 2,

$\underline{p_{B,1}, p_{B,2}, \ldots p_{B,k}}$ [$P_{B,1}, P_{B,2}, \ldots P_{B,k}$] are distinct random prime numbers,

e_B is relatively prime to

$\text{lcm}(p_{B,1}\text{-}1, p_{B,2}\text{-}1, \ldots p_{B,k}\text{-}1)$, and

d_B is selected from the group consisting of [the] a class of numbers equivalent to a multiplicative inverse of

e_B (mod(lcm(($p_{B,1}$-1), ($p_{B,2}$ -1), . . . , ($p_{B,k}$ -1)))), [wherein]said first terminal [comprises:] further having

blocking means for transforming a second message,[-to-be-transmitted] which is to be transmitted on said communications channel from said first terminal to said second terminal, to one or more transmit message word signals M_A, where each M_A corresponds to a number representative of said message in the range

[$0\leq M_A^{eB}$ (mod n_B)] $0\leq M_A \leq n_B$-1

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, [

]where C_A corresponds to a number representative of an encoded[enciphered] form of said second message [and corresponds to] through a relationship of the form

[$C_A \equiv M_A^{eB}$ (mod n_B)] $C_A \equiv M_A^{e_B} (\mathrm{mod}\, n_B)$

[wherein] said second terminal [comprises;] further having

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_A from said channel and for transforming each of said ciphertext word signals to a receive message word signal [M_A']M'_A, and

means for transforming said receive message word signals [M_A]M'_A to said message, [

]where [M'] M'_A corresponds to a number representative of a [deciphered] decoded form of C_A [and corresponds to] through a relationship of the form

[$M_A' \equiv C_A^{dB}$ (mod n_B)] $M'_A \equiv C_A^{d_B} (\mathrm{mod}\, n_B)$.

7. (Amended) A method [for establishing] of processing a message for use in cryptographic communications, comprising the steps of:

developing a composite number, n, as a product of at least 3 whole number factors greater than one, the factors being distinct random prime numbers; and encoding a digital message word signal M to a [cipher text] ciphertext word signal C, where said digital message word signal M corresponds to a number representative of a message and

$0\leq M\leq n-1$,

[where n is a composite number having at least 3 whole number factors greater than one, the factors being distinct prime numbers, and]

where said ciphertext word signal C corresponds to a number representative of an encoded form of said message [word M,] through a relationship of the form

[wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby]

$C\equiv a_e M^e + a_{e-1} M^{e-1} + \ldots + a_0 \pmod{n}$

where e and a_e, a_{e-1}, . . . , a_0 are numbers.

8. (Amended) [In the] A method according to claim 7 wherein said encoding step further includes the step of

transforming said digital message word signal M to said cipertext word signal C by the performance of a first ordered succession of inveritble operations on M, [the further step of:]

and wherein the method further comprises the step of:

decoding said cipertext word signal C to said digital message word signal M by the performance of a second ordered succession of invertible operations on C, where each of the invertible operations of said second ordered succession is the inverse of a corresponding one of said first ordered succession, and where[in] the order of said invertible operations in said second ordered succession is reversed with respect to the order of corresponding invertible operations in said first ordered succession.

9. (Amended) A communication system for [transferring] processing message signals [M_i], comprising:

[ ]j terminals including first and second terminals[stations], each of the j [stations]terminals being characterized by an encoding key $E_i = (e_i, n_i)$ and decoding key $D_i = (d_i, n_i)$[ ], where i=1,2, . . . ,j, [and wherein

M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal,] each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} terminal corresponds to an i^{th} message signal M_i, and

$0 \le M_i \le n_i - 1$,

n_i [is] being a composite number of the form

[$n_i = pi_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$] $n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to

$\mathrm{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots p_{i,k}-1)$, and

d_i is selected from the group consisting of the class of numbers equivalent

to a multiplicative inverse of

$e_i \,(\mathrm{mod}(\mathrm{lcm}((p_{i,1} -1), (p_{i,2} -1), \ldots, (p_{i,k} -1))))$;

said[a] first terminal [one of the j terminals] including

means for encoding a digital message word signal [M_A] M_1 [for transmission] to be transmitted from said first terminal (i=1[A]) to [a]said second terminal [one of the j terminals] (i=2[B]), said encoding means [for] transforming said digital message word signal [M_A]M_1 to a signed message word signal [M_{As}] M_{1s} using a relationship of the form [, M_{1s} corresponding to a number representative of an encoded form of said message word signal M_A,

whereby:]

$$[M_{As} \equiv M_A^{dA} (\mathrm{mod}\ n_A)]\, M_{1s} \equiv M_1^{d_1} (\mathrm{mod}\, n_1).$$

10. (Amended) The communication system of claim 9 further comprising:

means for transmitting said [signal]signed message word signal [M_{As}] M_{1s} from said first terminal to said second terminal, [and wherein]

said second terminal [includes] including

means for decoding said signed message word signal [M_{As}] M_{1s} to said digital message word signal [M_A,] M_1 using a relationship of the form [said second terminal including:]

$$M_1 \equiv M_{1s}^{e_1} (\bmod n_1)$$

[means for transforming said signed message word signal M_{As} to said message word signal M_A, whereby

$M_A \equiv M_{As}^{eA}$ (mod n_A)].

11. (Amended) A communications system for transferring a message signal [M_i], the communications system comprising:

[ ]j communication stations including first and second stations, each of the j communication stations being characterized by an encoding key E_i=(e_i, n_i) and a decoding key D_i =(d_i, n_i), where i=1, 2,. . . , j, [and wherein M_i corresponds to a number representative of a message signal to be transmitted from the ith terminal,] each of the j communication stations being adapted to transmit a particular one of the message signals where an ith communication station corresponds to an ith message signal M_i, and

$0 \leq M_i \leq n_i$-1

n_i [is] being a composite number of the form

$n_i = p_{i,1} \cdot p_{i,2} \cdot . . . \cdot p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}$, $p_{i,2}$, . . . ,$p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to $\mathrm{lcm}(p_{i,1} -1, p_{i,2} -1, \ldots, p_{i,k} -1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_i\ (\mathrm{mod}(\mathrm{lcm}((p_{i,1} -1), (p_{i,2} -1), \ldots, (p_{i,k} -1))))$,

[a]said first station [one of the j communication stations] including

means for encoding a digital message word signal [M_A] M_1 [for transmission] to be transmitted from said first station [one of the j communication stations] (i=1[A]) to [a] said second station [one of the j communication stations] (i=2[B]),

means for transforming said digital message word signal [M_A] M_1 to one or more message block word signals [M_A'] M_1'', each block word signal [M_A'] M_1'' being a number representative of a portion of said message word signal [M_A']M_1 in the range

$0\leq M_1''\leq n_2-1$ [$0\leq M_A \leq n_B -1$], and

means for transforming each of said message block word signals [M_A''] M_1'' to a ciphertext word signal C_1 using a relatinship of the form [C_A, C_A corresponding to a number representative of an encoded form of said message block word signal M_A'', whereby:]

$[C_A \equiv M_A''^{Eb}\ (\mathrm{mod}\ n_B)]\ C_1 \equiv M''^{e_2}_1\ (\mathrm{mod}\, n_2)$.

12. (Amended) The communications system of claim 11 further comprising:

means for transmitting said ciphertext word signals C_1 from said first [terminal] station to said second [terminal] station, [and]

wherein said second [terminal] station includes

means for decoding said ciphertext word signals C_1 to said message block word signals [MA] M_1'' using a relationship of the form[, said second terminal including:

means for transforming each of said ciphertext word signals C_A to one of said message block word signals M_A'', whereby

$M_A'' \equiv C_A^{Db}$ (mod n_B)] $M''_1 \equiv C_1^{d_2} (\bmod n_2)$, and

means for transforming said message block word signals [M_A''] M_1'' to said message word signal [M_A]M_1.

13. (Amended) [In a] A communications system, [including] comprising:

a first station; and

[and] a second [communicating] station[s inter]connected to the first station for communications therebetween,

the first communicating station having

encoding means for transforming a transmit message word signal M to a ciphertext word signal C where transmit message word signal M corresponds to a number representative of a message and

$0 \leq M \leq n\text{-}1$

[where] n [is] being a composite number formed as a product of [having] at least 3 whole number factors greater than one, the factors being distinct random prime numbers, and

where the ciphertext word signal C corresponds to a number representative of an [enciphered] encoded form of said message through a relationship of the form [and corresponds to]

$C \equiv a_e M^e + a_{e\text{-}1} M^{e\text{-}1} + \ldots + a_0 \text{ (mod } n)$

where e and a_e, a_{e-1}[-1], . . . , a_0 are numbers; and

means for transmitting the ciphertext word signal C to the second [communicating] station.

New Claims:

14. A method of processing a message for use in cryptographic communications comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

computing a composite number, n, as a product of the k distinct random prime numbers; and

encoding a plaintext message data M to a ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

15. The method according to claim 14, comprising the further step of:

establishing a private key portion d by a relationship to the public key portion e in the form of

$d \equiv e^{-1}(\bmod((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$; and

decoding the ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

16. A method of processing a message for use in cryptographic communications comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)));$$

computing a composite number, n, as a product of the k distinct random prime numbers;

obtaining a ciphertext message data C; and

decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M\equiv C^d$ (mod n).

17. The method according to claim 16, comprising the further step of:

encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C\equiv M^e$ (mod n), where $0\leq M\leq n$-1.

18. A method of processing a message for use in cryptographic communications comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e of the form

$$d \equiv e^{-1}(\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)));$$

computing a composite number, n, as a product of the k distinct random prime numbers;

encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s\equiv M^d$ (mod n), where $0\leq M\leq n$-1.

19. The method of claim 18 further comprising the step of:

decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M\equiv M_s^e$ (mod n).

20. A method for increasing the efficiency of a cryptographic process, comprising the steps of:

selecting a public key portion *e*;

developing *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion *e*;

computing a composite number, n, as a product of the k distinct random prime numbers; and

encoding a plaintext message data *M* to a ciphertext message data *C*, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

whereby a computational speed of the cryptographic process is increased.

21. The method according to claim 20, comprising the further step of:

establishing a private key portion *d* by a relationship to the public key portion *e* in the form of

$$d \equiv e^{-1}(\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))\text{; and}$$

decoding the ciphertext message data *C* to the plaintext message data *M* using a relationship of the form $M \equiv C^d \pmod{n}$.

22. A method for increasing the efficiency of a cryptographic process, comprising the steps of:

selecting a public key portion *e*;

developing *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion *e*;

establishing a private key portion *d* by a relationship to the public key portion *e* in the form of

$$d \equiv e^{-1}(\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))\text{;}$$

computing a composite number, n, as a product of the k distinct random prime numbers;

obtaining a ciphertext message data C; and

decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$,

whereby a computational speed of the cryptographic process is increased.

23. The method according to claim 22, comprising the further step of:

encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

24. The method according to claim 20, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

25. The method according to claim 22, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

26. The method according to claim 24, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

27. The method according to claim 25, wherein the developing, computing and encoding steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

28. The method according to claim 14, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

29. The method according to claim 28, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

30. The method according to claim 16, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

31. The method according to claim 30, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

32. The method according to claim 18, wherein p and q are a pair of prime numbers the product of which equals n, and wherein the k distinct random prime numbers are each smaller than p and q, whereby for a given length of n it takes fewer computational cycles to find and

check the K distinct random prime numbers that it takes to find and check the pair of prime numbers p and q.

33. The method according to claim 32, wherein the developing and computing steps can be performed for n that is more than 600 digits long faster than heretofore possible with only the pair of prime numbers p and q.

34. The method according to claim 14, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

35. The method according to claim 14, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

36. The method according to claim 16, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

37. The method according to claim 18, wherein a message processed in accordance with the method is compatible with two-prime RSA public key cryptography.

38. The method according to claim 20, wherein message data processed in accordance with the method is compatible with two-prime RSA public key cryptography.

39. The method according to claim 22, wherein message data processed in accordance with the method is compatible with two-prime RSA public key cryptography.

40. A cryptography method for local storage of data by a private key owner, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of

$$d \equiv e^{-1}(\mathrm{mod}((p_1 - 1)\cdot(p_2 - 1)\cdots(p_k - 1)));$$

computing a composite number, n, as a product of the k distinct random prime numbers that are factors of n, where only the private key owner knows the factors of n;

encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

41. The cryptography method in accordance with claim 40, further comprising the step of:

decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d \pmod{n}$.

42. A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to conduct encrypted communications with the plurality of stations via the communications medium, the host system including

at least one cryptosystem responsive to encryption and/or decryption requests from the host system, the cryptosystem being configured for

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to a public key portion e that is associated with the host system, computing a composite number, n, as a product of the k distinct random prime numbers,

encoding a plaintext message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\bmod((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$; and

decoding a ciphertext message data C' communicated via the host producing therefrom a plaintext message data M' using a relationship of the form $M' \equiv C'^{d} \pmod{n}$, where C' and M' can be respectively C and M.

43. A system for processing a message used in cryptographic communications, comprising:

a bus; and

a cryptosystem operatively coupled to and receiving from the bus encryption and decryption requests, the cryptosystem being capable of

providing a public key portion e,

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e,

computing a composite number, n, as a product of the k distinct random prime numbers,

encoding a plaintext form of a first message M to produce a ciphertext form of the first message C using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\bmod((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$, and decoding the ciphertext form of a second message C' to produce the plaintext form of the second message M' using a relationship of the form $M' \equiv C'^{d}$ (mod n), the first and second messages can be one and the same.

44. The system of claim 42, wherein the at least one cryptosystem includes

a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

45. The system of claim 42, wherein the at least one cryptosystem includes

a processor,

a data-address bus,

a memory operatively coupled to the processor via the data-address bus,

a data encryption standard (DES) unit operatively coupled the memory and the processor via the data-address bus,

a plurality of exponentiator elements operatively coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. The system of claim 45, wherein the memory and each of the plurality of exponentiator elements has its own DES unit that encrypts message data received/returned from/to the processor.

47. The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor including secure, insecure and exponentiator elements address spaces, and wherein the DES unit that is coupled to the processor is configured to recognize the secure and exponentiator elements address spaces and to automatically encrypt message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when

the processor is accessing the insecure memory address spaces, the DES unit being further configured to decrypt encrypted message data received from the memory before it is provided to the processor.

48. The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

49. The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors $p_1, p_2, \ldots p_k$.

50. A system for processing a message used in cryptographic communications, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encryption and decryption requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encryption and decryption requests, each encryption request providing a plaintext message M to be encrypted, each encryption request can additionally provide a public key that includes an exponent e and a representation of a modulus n in the form of its k distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$, or the processor can obtain the public key from the memory,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $C_1, C_2, \ldots C_k$, and

forming a ciphertext message C from the subtask values $C_1, C_2, \ldots C_k$.

51. The system of claim 50 wherein each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\bmod p_i)$, where $M_i \equiv M(\bmod p_i)$, and $e_i \equiv e(\bmod p_i - 1)$, where i=1, 2, ... k.

52. A system for processing a message used in cryptographic communications, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encryption and decryption requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encryption and decryption requests, each encryption/decryption request providing a plaintext/ciphertext message *M/C* to be encrypted/decrypted and can additionally provide a public/private key that includes an exponent *e/d* and a representation of a modulus *n* in the form of its *k* distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$, or the processor can obtain the public/private key from the memory,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $M_1, M_2, \ldots M_k/C_1, C_2, \ldots C_k$, and

forming the ciphertext/plaintext message *C/M* from the subtask values $C_1, C_2, \ldots C_k/M_1, M_2, \ldots M_k$.

53. The system of claim 52 wherein when produced each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{e_i} (\bmod p_i)$, where $C_i \equiv C(\bmod p_i)$, and $e_i \equiv e(\bmod p_i - 1)$, where i=1, 2, ... k.

54. The system of claim 52 wherein when produced each one of the subtasks $M_1, M_2, \ldots M_k$ is developed using a relationship of the form $M_i \equiv C_i^{d_i} (\mathrm{mod}\, p_i)$, where $M_i \equiv M (\mathrm{mod}\, p_i)$, and $d_i \equiv d(\mathrm{mod}\, p_i - 1)$, where i=1, 2, ... k.

55. The system of claim 54, wherein the private key exponent d relates to the public key exponent e via $d \equiv e^{-1}(\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$.

56. A system for processing a message used in cryptographic communications, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1 - 1) \cdot (p_2 - 1) \cdots (p_k - 1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers;

means for obtaining a ciphertext message data C; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d$ (mod n).

57. The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C \equiv M^e$ (mod n), where $0 \leq M \leq n$-1.

58. A system for processing a message used in cryptographic communications, comprising:

means for selecting a public key portion *e*;

means for developing *k* distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, . . . p_k-1, is relatively prime to the public key portion *e*;

means for establishing a private key portion *d* by a relationship to the public key portion *e* of the form $d \equiv e^{-1}(\bmod((p_1 - 1)\cdot(p_2 - 1)\cdots(p_k - 1)))$;

means for computing a composite number, *n*, as a product of the k distinct random prime numbers;

means for encoding a plaintext message data *M* with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d$ (mod *n*), where $0 \leq M \leq n$-1.

59. The system of claim 58 further comprising the step of:

means for decoding the signed message M_s with the private key portion e to produce the plaintext message data *M* using a relationship of the form $M \equiv M_s^e$ (mod *n*).

60. The system of claim 57, wherein the system can conduct encrypted communications with other public key cryptography system that encrypt/decrypt data using a modulus value equal to *n* independent of the *k* distinct prime numbers.

61. The system of claim 59, wherein the system can conduct encrypted communications with other public key cryptography systems that encrypt/decrypt data using a modulus value equal to *n* independent of the *k* distinct prime numbers.

REMARKS

This Preliminary Amendment is filed concurrently with a Reissue Application for U.S. Patent No. 5,848,159 (hereafter the "original patent").

Status of the Claims:

As of the date of this Preliminary Amendment, claims 1-13 of the original patent are amended and remain pending; claims 14-61 have been added. Thus, claims 1-61 are now pending in the Reissue Application.

Statement of Support in the Disclosure of the Original Patent for the Amendments:

The Specification:

The specification of the original patent has been amended to correct typographical errors and other matters of form and to render the specification consistent throughout and with the claims. Support for the amendments to the specification may be found throughout the original patent. No new matter has been introduced by the amendments to the specification.

In general, changes embodying corrections of typographical errors and other matters of form are self explanatory and need no further explanation. As to the mathematical expressions, equations expressing any congruence of the form $b=c(\text{mod } m)$ or the like, where b is congruent to c and m is the modulus, are mathematically written in proper form as $b\equiv c(\text{mod } m)$. Accordingly all the equations are written in proper form, e.g., $C\equiv M^e(\text{mod } n)$. Were applicable, the parentheses (e.g., around "mod n") are properly added as well.

Support for amendments to the paragraph beginning at column (hereafter "col."), line 4 may be found in col. 1 of the cover page. Support for the amendments to the paragraph beginning at col. 3, line 23 and the paragraph beginning at col. 3, line 27 may be found for example at col. 2 of the cover page and col. 13, lines 44-47.

Support for amendments to the paragraph beginning at col. 3, line 36, may be found at column 5, lines 31-33. Support for amendments to the paragraph beginning at col. 3, line 56, may be found for example at col. 3, lines 20-26, col. 3, lines 44-55 and col. 4, lines 9-11. Support for amendments to the paragraph beginning at col. 4, line 6, may be found for example at col. 3,lines 20-26, col. 4, lines 6-12, 32-34 and 52-56.

Support for amendments to the paragraph beginning at col. 4, line 13 and the paragraph beginning at col. 4, line 50, may be found for example at col. 3 line 42, col. 4, line 41, and col. 10, lines 54-56. Further support for amendments to the paragraph beginning at col. 4, line 50 may be found at col. 4, lines 50-52.

Support for paragraph inserted before the paragraph beginning at col. 5, line 52, may be found for example at col. 14, lines 30-36 and 45-49. Support for amendments to the paragraph beginning at col. 5, line 30, may be found for example at col. 2, lines 5-10, col. 3, line 42, col. 4 line 41, col. 5, line 39, col. 10, line 65 and col. 11, lines 8-9. Further support for amendments to the paragraph beginning at col. 5, line 30, may be found in the multitude of mathematical expressions where d, the private key portion, is the "exponent," e.g., $M \equiv C^d$(mode n) at col. 6, lines 1-5.

Support for amendments to the paragraph beginning at col. 6, line 24, may be found for example at col. 5, lines 31-33, col. 6, line 37 ("M=Y_k..."), col. 7, line 15, and col. 11, lines 15-20. Support for amendments to the paragraph beginning at col. 6, line 65, may be found for example at col. 6, lines 1-4, 26-35, 40-53 and 67. Support for amendments to the paragraph beginning at col. 7, line 1, may be found for example at col. 2, lines 32-34 and 40, col. 3, lines 22-26, col. 4, lines 32-34, col. 6 line 38 and col. 7, lines 56-58.

Support for amendments to the paragraph beginning at col. 8, line 1, is fund in col. 8 line 3 (i.e., FIPS 140-1 with level 3 is a well known standard, See: http://csrc.nist.gov/fips/fips1401.htm). Support for amendments to the paragraph beginning at col. 10, line 15, may be found for example at Figure 3. Support for amendments to the paragraph beginning at col. 10, line 35, may be found for example in col. 10 line 40 and line 53 (i.e., M is represented by a numerical value greater than *0* and smaller than *n*).

The Claims:

Claims 1-13 of the original patent have been amended to correct typographical errors and other matters of form, as well as to recite more clearly and particularly the subject matter which Applicants regard as their invention. New claims 14-61 have been added to further point out and distinctly claim subject matter which Applicants regard as their invention. Support for the amendments to claims 1-13 and for the newly added claims, 14-61, may be found throughout the original patent. No new matter has been introduced by the amendments to the claims.

In general, claim amendments embodying corrections of typographical errors, antecedent basis errors, and other matters of form are self explanatory and need no further explanation. As to the mathematical expressions, equations expressing any congruence of the form $b= c(\text{mod } m)$ or the like, where b is congruent to c and m is the modulus, are mathematically written in proper form as $b\equiv c(\text{mod } m)$. Accordingly all the equations are written in proper form, e.g., $C\equiv M^e(\text{mod } n)$. Were applicable, parentheses (e.g., around "mod n") are properly added as well.

Support for amendments to claim 1 as now presented may be found, for example, at claim 1 as presented in the original patent, as well as col.1, lines 32-42, col. 3, lines 39-44, col. 5, lines 30-33, col. 7, lines 25-28 and col. 8, lines 8-11. Support for amendments to claim 2 as now presented may be found, for example, at claims 1 and 2 as presented in the original patent, as well as col. 2, lines 24-30, col. 5, lines 36-40 and col. 14, lines 19-24. Similarly, support for amendments to claims 3-13 as now presented may be found, for example, at claims 1-13 as presented in the original patent. Further support for the amendments to claims 3-13 as now presented may be found for example at col.1, lines 32-42, col. 2, lines 24-30, col. 3, lines 39-44, col. 5, lines 30-40, col. 7, lines 25-28, col. 8, lines 8-11, and col. 14, lines 19-24. Further support for amendments to claim 12 as now presented may be found for example at col.9, lines 48-50.

As to the newly added claims, support for claim 14-23, 40-43, and 50-58 may be found, for example, at col. 1, lines 32-42, col.3, lines 35-44, col. 4, lines 37-49, col. 5, lines 30-33 and 36-51, col. 7, lines 25-28, col. 8, lines 8-11, col. 14, lines 30-36. Further support for new claims 14-23, 40-43, and 50-58 may be found at claims 1-13 as presented in the original patent. For example, support for new claims 18 and 19 may be found in claim 9, i.e., col. 14, lines 30-36. Further support for new claims 20 and 22 may be found at col. 3, lines 30-36 and 53-55, and col. 7, lines 25-28. Support for new claims 24-33 may be found for example at column 3, lines 36-65.

Support for new claims 34-39 may be found for example at col. 4, lines 8-12 and col. 5, lines 61-63. Further support for new claims 40 and 41 may be found at col. 5, lines 58-61. Further support for new claims 42, 43, 50-52, and support for new claims 44-49 may be found at Figures 1-3, and the accompanying description at col. 7, line 34 to col. 10, lines 34. Further support for new claims 50-54 may be found at col. 5, line 52 to col. 6, line 6. Finally, support for claims 60 and 61 may be found at col. 4, lines 6-13 and col. 5, lines 61-63.

Summary:

Entry of the foregoing amendments to the specification and claims is hereby respectfully requested. Claims 1-61 are now presented for examination in the Reissue Application which is believed to be in condition for allowance. Prompt examination and allowance of the pending claims is therefore respectfully requested.

Concurrent Office Proceedings; and Petition for Waiver of Delay:

It is noted that Reexamination Requests respecting the original patent have been filed with the U.S. Patent and Trademark Office on May 18, 2000 (Order Granting Reexamination mailed July 19, 2000; Control No. 90/005,733) and on July 28, 2000, respectively. In view of the concurrent office proceedings, Reexamination and Reissue Application, it is hereby requested that the Reexamination proceeding be stayed until the Reissue Application proceeding is concluded, or, in the alternative, that the Reexamination proceeding be merged with the Reissue Application proceeding (37 C.F.R. 1.565(d)).

In view of the concurrent office proceedings, a Petition under 37 C.F.R. 1.183 to waive the 2-months delay for protest is attached herewith. Examination of the Reissue Application should commence without delay and before the Reexamination proceeds.

Fee Authorization:

If for any reason an insufficient fee has been paid, the Commissioner is hereby authorized to charge any deficiency in payment of required fees associated with this communication to Deposit Account **02-3964.**

Date: October 19, 2000

Respectfully submitted,

By: Leah Sherry,
Attorney for Applicant
Reg. No. 43,918

Oppenheimer Wolff & Donnelly LLP
3373 Hillview Avenue
Palo Alto, CA 94304
Tel: (650) 320-4000

CERTIFICATE OF MAILING (37 CFR 1.10(a))

CERTIFICATE OF MAILING BY "EXPRESS MAIL" - Rule 10: I hereby certify that this correspondence is being deposited on October 5, 2000 with the U.S. Postal Service "Express Mail Post Office to Addressee" under 37 CFR 1.10 as **Express Mail No. EL655031318US** addressed to: Box Reissue Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231

Date: October 19, 2000

PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD

This application claims the benefit of U.S. Provisional Application No. 60/033.271 for PUBLIC KEY CRYTOGRAPHIC APPARATUS AND METHOD. filed Dec. 9. 1996. naming as inventors. Thomas Colins. Dale Hopkins. Susan Langford and Michale Sabin. the discolsure of which is incorporated by reference.

BACKGROUND OF THE INVENTION

This invention relates generally to communicating data in a secure fashion. and more particularly to a cryptographic system and methods using public key cryptography.

Computer systems are found today in virtually every walk of life for storing. maintaining. and transferring various types of data. The integrity of large portions of this data. especially that portion relating to financial transactions. is vital to the health and survival of numerous commercial enterprises. Indeed. as open and unsecured data communications channels for sales transactions gain popularity. such as credit card transactions over the Internet. individual consumers have an increasing stake in data security.

Thus. for obvious reasons. it is important that financial transaction communications pass from a sender to an intended receiver without intermediate parties being able to interpret the transferred message.

Cryptography. especially public key cryptography. has proven to be an effective and convenient technique of enhancing data privacy and authentication. Data to be secured. called plaintext. is transformed into encrypted data. or ciphertext. by a predetermined encryption process of one type or another. The reverse process. transforming ciphertext into plaintext. is termed decryption. Of particular importance to this invention is that the processes of encryption and decryption are controlled by a pair of related cryptographic keys. A "public" key is used for the encryption process. and a "private" key is used to decrypt ciphertext. The public key transforms plaintext to ciphertext. but cannot be used to decrypt the ciphertext to retrieve the plaintext therefrom.

As an example. suppose a Sender A wishes to send message M to a recipient B. The idea is to use public key E and related private key D for encryption and decryption of M. The public key E is public information while D is kept secret by the intended receiver. Further. and importantly. although E is determined by D. it is extremely difficult to compute D from E. Thus the receiver. by publishing the public key E. but keeping the private key D secret. can assure senders of data encrypted using E that anyone who intercepts the data will not be able to decipher it. Examples of the public key/private key concept can be found in U.S. Pat. Nos. 4.200.770. 4.218.582. and 4.424.414.

The prior art includes a number of public key schemes. in addition to those described in the above-identified patents. Over the past decade. however. one system of public key cryptography has gained popularity. Known generally as the "RSA" scheme. it is now thought by many to be a worldwide defacto standard for public key cryptography. The RSA scheme is described in U.S. Pat. No. 4.405.829 which is fully incorporated herein by this reference.

The RSA scheme capitalizes on the relative ease of creating a composite number from the product of two prime numbers whereas the attempt to factor the composite number into its constituent primes is difficult. The RSA scheme uses a public key E comprising a pair of positive integers n and e. where n is a composite number of the form

$$n=p\cdot q \qquad (1)$$

where p and q are different prime numbers. and e is a number relatively prime to (p−1) and (q−1): that is. e is relatively prime to (p−1) or (q−1) if e has no factors in common with either of them. Importantly. the sender has access to n and e. but not to p and q. The message M is a number representative of a message to be transmitted wherein

$$0 \leqq M < n-1. \qquad (2)$$

The sender enciphers M to create ciphertext C by computing the exponential

$$C=M^e (\text{mod } n). \qquad (3)$$

The recipient of the ciphertext C retrieves the message M using a (private) decoding key D. comprising a pair of positive integers d and n. employing the relation

$$M=C^d (\text{mod } n) \qquad (4)$$

As used in (4). above. d is a multiplicative inverse of

$$e(\text{mod}(\text{lcm}((p-1), (q-1)))) \qquad (5)$$

so that

$$e\cdot d=1(\text{mod}(\text{lcm}((p-1), (q-1)))) \qquad (6)$$

where lcm((p−1). (q−1)) is the least common multiple of numbers p−1 and q−1. Most commercial implementations of RSA employ a different. although equivalent. relationship for obtaining d:

$$d=e^{-1} \text{mod}(p-1)\ (q-1). \qquad (7)$$

This alternate relationship simplifies computer processing.

Note: Mathematically (6) defines a set of numbers and (7) defines a subset of that set. For implementation. (7) or (6) usually is interpreted to mean d is the smallest positive element in the set.)

The net effect is that the plaintext message M is encoded knowing only the public key E (i.e.. e and n). The resultant ciphertext C can only decoded using decoding key D. The composite number n. which is part of the public key E. is computationally difficult to factor into its components. prime numbers p and q. a knowledge of which is required to decrypt C.

From the time a security scheme. such as RSA. becomes publicly known and used. it is subjected to unrelenting attempts to break it. One defense is to increase the length (i.e.. size) of both p and q. Not long ago it was commonly recommended that p and q should be large prime numbers 75 digits long (i.e.. on the order of 10^{75}). Today. it is not uncommon to find RSA schemes being proposed wherein the prime numbers p and q are on the order of 150 digits long. This makes the product of p and q a 300 digit number. (There are even a handful of schemes that employ prime numbers (p and q) that are larger. for example 300 digits long to form a 600 digit product.) Numbers of this size. however. tend to require enormous computer resources to perform the encryption and decryption operations. Consider that while computer instruction cycles are typically measured in nanoseconds (billionths of seconds). computer computations of RSA steps are typically measured in milliseconds (thousandths of seconds). Thus millions of computer cycles are required to compute individual RSA steps resulting in noticeable delays to users.

This problem is exacerbated if the volume of ciphertext messages requiring decryption is large—such as can be expected by commercial transactions employing a mass communication medium such as the Internet. A financial institution may maintain an Internet site that could conceivably receive thousands of enciphered messages every hour that must be decrypted. and perhaps even responded to. Using larger numbers to form the keys used for an RSA scheme can impose severe limitations and restraints upon the institution's ability to timely respond.

Many prior art techniques. while enabling the RSA scheme to utilize computers more efficiently. nonetheless have failed to keep pace with the increasing length of n. p. and q.

Accordingly. it is an object of this invention to provide a system and method for rapid encryption and decryption of data without compromising data security.

It is another object of this invention to provide a system and method that increases the computational speed of RSA encryption and decryption techniques.

It is still another object of this invention to provide a system and method for implementing an RSA scheme in which the components of n do not increase in length as n increases in length.

It is still another object to provide a system and method for utilizing multiple (more than two). distinct prime number components to create n.

It is a further object to provide a system and method for providing a technique for reducing the computational effort for calculating exponentiations in an RSA scheme for a given length of n.

SUMMARY OF THE INVENTION

The present invention discloses a method and apparatus for increasing the computational speed of RSA and related public key schemes by focusing on a neglected area of computation inefficiency. Instead of n=p·q. as is universal in the prior art. the present invention discloses a method and apparatus wherein n is developed from three or more distinct prime numbers; i.e.. $n=p_1 \cdot p_2 \cdot \ldots \cdot p_k$. where k is an integer greater than 2 and $p_1, p_2, \ldots p_k$ are sufficiently large distinct primes. Preferably. "sufficiently large primes" are prime numbers that are numbers approximately 150 digits long or larger. The advantages of the invention over the prior art should be immediately apparent to those skilled in this art. If. as in the prior art. p and q are each on the order of. say. 150 digits long. then n will be on the order of 300 digits long. However. three primes p_2. p_1. and p_3 employed in accordance with the present invention can each be on the order of 100 digits long and still result in n being 300 digits long. Finding and verifying 3 distinct primes. each 100 digits long. requires significantly fewer computational cycles than finding and verifying 2 primes each 150 digits long.

The commercial need for longer and longer primes shows no evidence of slowing: already there are projected requirements for n of about 600 digits long to forestall incremental improvements in factoring techniques and the ever faster computers available to break ciphertext. The invention. allowing 4 primes each about 150 digits long to obtain a 600 digit n. instead of two primes about 350 digits long. results in a marked improvement in computer performance. For. not only are primes that are 150 digits in size easier to find and verify than ones on the order of 350 digits. but by applying techniques the inventors derive from the Chinese Remainder Theorem (CRT). public key cryptography calculations for encryption and decryption are completed much faster—even if performed serially on a single processor system. However, the inventors' techniques are particularly adapted to be advantageously apply enable public key operations to parallel computer processing.

The present invention is capable of using the RSA scheme to perform encryption and decryption operation using a large (many digit) n much faster than heretofore possible. Other advantages of the invention include its employment for decryption without the need to revise the RSA public encryption transformation scheme currently in use on thousands of large and small computers.

A key assumption of the present invention is that n. composed of 3 or more sufficiently large distinct prime numbers. is no easier (or not very much easier) to factor than the prior art. two prime number n. The assumption is based on the observation that there is no indication in the prior art literature that it is "easy" to factor a product consisting of more than two sufficiently large. distinct prime numbers. This assumption may be justified given the continued effort (and failure) among experts to find a way "easily" to break large component numbers into their large prime factors. This assumption is similar. in the inventors' view. to the assumption underlying the entire field of public key cryptography that factoring composite numbers made up of two distinct primes is not "easy." That is. the entire field of public key cryptography is based not on mathematical proof. but on the assumption that the empirical evidence of failed sustained efforts to find a way systematically to solve NP problems in polynomial time indicates that these problems truly are "difficult."

The invention is preferably implemented in a system that employs parallel operations to perform the encryption. decryption operations required by the RSA scheme. Thus. there is also disclosed a cryptosystem that includes a central processor unit (CPU) coupled to a number of exponentiator elements. The exponentiator elements are special purpose arithmetic units designed and structured to be provided message data M. an encryption key e. and a number n (where $n=p_1*p_2* \ldots p_k$. k being greater than 2) and return ciphertext C according to the relationship.

$$C=M^e(\text{mod}(n)).$$

Alternatively. the exponentiator elements may be provided the ciphertext C. a decryption (private) key d and n to return M according to the relationship.

$$M=C^d(\text{mod}(n))$$

According to this aspect of the invention. the CPU receives a task. such as the requirement to decrypt cyphertext data C. The CPU will also be provided. or have available. a public key e and n. and the factors of n (p_1. p_2. . . . p_k). The CPU breaks the encryption task down into a number of sub-tasks. and delivers the sub-tasks to the exponentiator elements. When the results of the sub-tasks are returned by the exponentiator elements to the CPU which will. using a form of the CRT. combine the results to obtain the message data M. An encryption task may be performed essentially in the same manner by the CPU and its use of the exponentiator elements. However. usually the factors of n are not available to the sender (encryptor). only the public key. e and n. so that no sub-tasks are created.

In a preferred embodiment of this latter aspect of the invention. the bus structure used to couple the CPU and exponentiator elements to one another is made secure by encrypting all important information communicated thereon. Thus. data sent to the exponentiator elements is passed through a data encryption unit that employs. preferably. the ANSI Data Encryption Standard (DES). The exponentiator elements decrypt the DES-encrypted sub-task information they receive. perform the desired task. and encrypt the result. again using DES. for return to the CPU.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a simplified block diagram of a cryptosystem architecture configured for use in the present invention.

FIG. 2 is a memory map of the address space of the cryptosystem of FIG. 1; and

FIG. 3 is an exemplary illustration of one use of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

As indicated above. the present invention is employed in the context of the RSA public key encryption/decryption scheme. As also indicated. the RSA scheme obtains its security from the difficulty of factoring large numbers. and the fact that the public and private keys are functions of a pair of large (100–200 digits or even larger) prime numbers. Recovering the plaintext from the public key and the ciphertext is conjectured to be equivalent to factoring the product of two primes.

According to the present invention. the public key portion e is picked. Then. three or more random large. distinct prime numbers. p_1. p_2. . . . . p_k are developed and checked to ensure that each is relatively prime to e. Preferably. the prime numbers are of equal length. Then. the product n=p_1. p_2. . . . . p_k is computed.

Finally. the decryption key. d. is established by the relationship:

$$d=e^{-1} \bmod ((p_1-1)(p_2-1)\ .\ .\ (p_k-1))$$

The message data. M is encrypted to ciphertext C using the relationship of (3). above. i.e..

$$C=M^e \bmod n.$$

To decrypt the ciphertext. C. the relationship of (3). above. is used:

$$M=C^d \bmod n$$

where n and d are those values identified above.

Using the present invention involving three primes to develop the product n. RSA encryption and decryption time can be substantially less than an RSA scheme using two primes by dividing the encryption or decryption task into sub-tasks. one sub-task for each distinct prime. (However. breaking the encryption or decryption into subtasks requires knowledge of the factors of n. This knowledge is not usually available to anyone except the owner of the key. so the encryption process can be accelerated only in special cases. such as encryption for local storage. A system encrypting data for another user performs the encryption process according to (3). independent of the number of factors of n. Decryption. on the other hand. is performed by the owner of a key. so the factors of n are generally known and can be used to accelerate the process.) For example. assume that three distinct primes. p_1. p_2. and p_3. are used to develop the product n. Thus. decryption of the ciphertext. C. using the relationship

$$M=C^d(\text{mod } n)$$

is used to develop the decryption sub-tasks:

$$M_1=C_1^{d_1}\text{mod } p_1$$

$$M_2=C_2^{d_2}\text{mod } p_2$$

$$M_3=C_3^{d_3}\text{mod } p_3$$

where

$$C_1=C\text{mod } p_1;$$

$$C_2=C\text{mod } p_2;$$

$$C_3=C\text{mod } p_3;$$

$$d_1=d\text{mod } (p_1-1);$$

$$d_2=d\text{mod } (p_2-1); \text{ and}$$

$$d_3=d\text{mod } (p_3-1).$$

The results of each sub-task. M_1. M_2. and M_3 can be combined to produce the plaintext. M. by a number of techniques. However. it is found that they can most expeditiously be combined by a form of the Chinese Remainder Theorem (CRT) using. preferably. a recursive scheme. Generally. the plaintext M is obtained from the combination of the individual sub-tasks by the following relationship:

$$Y_i=Y_{i-1}+[(M_i-Y_{i-1})\ (w_i^{-1}\text{mod } p_i)\text{mod } p_i]\cdot w_i\text{mod } n$$

where

$$i\geqq 2 \text{ and}$$

$$M = Y_k,\ Y_1 = C_1, \text{ and } w_i = \prod_{j<i} p_j$$

Encryption is performed in much the same manner as that used to obtain the plaintext M. provided (as noted above) the factors of n are available. Thus. the relationship

$$C=M^e(\text{mod } n),$$

can be broken down into the three sub-tasks.

$$C_1=M_1^{e_1}\text{mod } p_1$$

$$C_2=M_2^{e_2}\text{mod } p_2$$

$$C_3=M_3^{e_3}\text{mod } p_3$$

where

$$M_1=M(\text{mod } p_1),$$

$$M_2=M(\text{mod } p_2),$$

$$M_3=M(\text{mod } p_3),$$

$$e_1=e\text{mod } (p_1-1),$$

$$e_2=e\text{mod } (p_2-1), \text{and}$$

$$e_3=e\text{mod } (p_3-1)$$

In generalized form. the decrypted message M can be obtained by the same summation identified above to obtain the ciphertext C from its contiguous constituent sub-tasks C_i.

Preferably. the recursive CRT method described above is used to obtain either the ciphertext. C. or the deciphered plaintext (message) M due to its speed. However. there may be occasions when it is beneficial to use a non-recursive technique in which case the following relationships are used:

$$M = \sum_{i=1}^{k} M_i(w_i^{-1} \, mod \, p_i)w_i \, mod \, n$$

where

$$w_i = \prod_{j \neq 1} p_j, \text{ and}$$

k is the number (3 or more) of distinct primes chosen to develop the product n.

Thus. for example above (k=3). M is constructed from the returned sub-task values M_1. M_2. M_3 by the relationship

$$M=M_1(w_1^{-1}\text{mod } p_1)\, w_1\text{mod/n}+M_2(w_2^{-1}\text{mod } p_2)\, w_2\text{mod } n+M_3(w_3^{-1}\text{mod } p_3)\, w_3\text{mod } n$$

where

$$w_1=p_2p_3,\ w_2=p_1p_3, \text{ and } w_3=p_1p_2.$$

Employing the multiple distinct prime number technique of the present invention in the RSA scheme can realize accelerated processing over that using only two primes for the same size n. The invention can be implemented on a single processor unit or even the architecture disclosed in the above-referenced U.S. Pat. No. 4.405.829. The capability of developing sub-tasks for each prime number is particularly adapted to employing a parallel architecture such as that illustrated in FIG. 1.

Turning to FIG. 1. there is illustrated a cryptosystem architecture apparatus capable of taking particular advantage of the present invention. The cryptosystem. designated with the reference numeral **10**. is structured to form a part of a larger processing system (not shown) that would deliver to the cryptosystem **10** encryption and/or decryption requests. receiving in return the object of the request—an encrypted or decrypted value. The host would include a bus structure **12**. such as a peripheral component interface (PCI) bus for communicating with the cryptosystem **10**.

As FIG. **1** shows. The cryptoprocessor **10** includes a central processor unit (CPU) **14** that connects to the bus structure **12** by a bus interface **16**. The CPU **14** comprises a processor element **20**. a memory unit **22**. and a data encryption standard (DES) unit **24** interconnected by a data/address bus **26**. The DES unit **24**. in turn. connects to an input/output (I/O) bus **30** (through appropriate driver/receiver circuits—not shown).

The I/O bus **30** communicatively connects the CPU to a number of exponentiator elements $\mathbf{32}_a$. $\mathbf{32}_b$. and $\mathbf{32}_c$. Shown here are three exponentiator elements. although as illustrated by the "other" exponentiators $\mathbf{32}_n$. additional exponentiator elements can be added. Each exponentiator element is a state machine controlled arithmetic circuit structured specifically to implement the relationship described above. Thus. for example. the exponentiator **32***a* would be provided the values M_1. e_1. and p. n to develop C_1. Similarly. the exponentiator circuits **32***b* and **32***c* develop C_2 and C_3 from corresponding subtask values M_2. e_2. P_2. M_3. e_3. and P_3.

Preferably. the CPU **14** is formed on a single integrated circuit for security reasons. However. should there be a need for more storage space than can be provided by the "on-board" memory **22**. the bus **30** may also connect the CPU **14** to an external memory unit **34**.

In order to ensure a secure environment. it is preferable that the cryptosystem **10** meet the Federal Information Protection System (FIPS) level 3. Accordingly. the elements that make up the CPU **14** would be implemented in a design that will be secure from external probing of the circuit. However. information communicated on the I/O bus **30** between the CPU **14** and the exponentiator circuits **32** (and external memory **34**—if present) is exposed. Consequently. to maintain the security of that information. it is first encrypted by the DES unit **24** before it is placed on the I/O bus **30** by the CPU **14**. The exponentiator circuits **32**. as well as the external memory **34**. will also include similar DES units to decrypt information received from the CPU. and later to encrypt information returned to the CPU **14**.

It may be that not all information communicated on the I/O bus **30** need be secure by DES encryption. For that reason. the DES unit **24** of the CPU **14** is structured to encrypt outgoing information. and decrypt incoming information. on the basis of where in the address space used by the cryptosystem the information belongs: that is. since information communicated on the I/O bus **30** is either a write operation by the CPU **14** to the memory **34**. or a read operation of those elements. the addresses assigned to the secure addresses and non-secure addresses. Read or write operations conducted by the CPU **14** using secure addresses will pass through the DES unit **24** and that of the memory **34**. Read or write operations involving non-secure addresses will by-pass these DES units.

FIG. 2 diagrammatically illustrates a memory map **40** of the address space of the cryptosystem **10** that is addressable by the processor **20**. As the memory map **40** shows. an address range **40** provides addresses for the memory **22**. and such other support circuitry (e.g.. registers—not shown) that may form a part of the CPU **14**. The addresses used to write information to. or read information from. the exponentiator elements **32** are in the address range **44** of the memory map **40**. The addresses for the external memory **34** are in the address ranges **46**. and **48**. The address ranges **44** and **46** are for secure read and write operations. Information that must be kept secure. such as instructions for implementing algorithms. encryption/decryption keys. and the like. if maintained in external memory **34**. will be stored at locations having addresses in the address range **46**. Information that need not be secure such as miscellaneous algorithms data. general purpose instructions. etc. are kept in memory locations of the external memory **34** having addresses within the address range **48**.

The DES unit **24** is structured to recognize addresses in the memory spaces **44**. **46**. and to automatically encrypt the information before it is applied to the I/O bus **30**. The DES unit **24** is bypassed when the processor **20** accesses addresses in the address range **48**. Thus. when the processor **20** initiates write operations to addresses within the memory space within the address range **46** (to the external memory **34**). the DES unit **24** will automatically encrypt the information (not the addresses) and place the encrypted information on the I/O bus **30**. Conversely. when the processor **20** reads information from the external memory **34** at addresses within the address range **46** of the external memory **34**. the DES unit will decrypt information received from the I/O bus **30** and place the decrypted information on the data/address bus **26** for the processor **20**.

In similar fashion. information conveyed to or retrieved from the exponentiators **32** by the processor **20** by write or read operations at addresses within the address range **44**. Consequently. writes to the exponentiators **32** will use the DES unit **24** to encrypt the information. When that (encrypted) information is received by the exponentiators

32. it is decrypted by on-board DES units (of each exponentiator 32). The results of the task performed by the exponentiator 32 is then encrypted by the exponentiator's on-board DES unit. retrieved by the processor **20** in encrypted form and then decrypted by the DES unit **24**.

Information that need not be maintained in secure fashion to be stored in the external memory **34**. however. need only be written to addresses in the address range **48**. The DES unit **24** recognizes writes to the address range **48**. and bypasses the encryption circuitry. passing the information. in unencrypted form. onto the I/O bus **30** for storing in the external memory **34**. Similarly. reads of the external memory **34** using addresses within the address range **48** are passed directly from the I/O bus **30** to the data/address bus **26** by the DES unit **24**.

In operation. the CPU **14** will receive from the host it serves (not shown). via the bus **12**. an encryption request. The encryption request will include the message data M to be encrypted and. perhaps. the encryption keys e and n (in the form of the primes p_1. p_2. . . . p_k). Alternatively. the keys may be kept by the CPU **14** in the memory **22**. In any event. the processor **20** will construct the encryption sub-tasks C_1. C_2. . . . . C_k for execution by the exponentiators **32**.

Assume. for the purpose of the remainder of this discussion. that the encryption/decryption tasks performed by the cryptosystem **10**. using the present invention. employs only three distinct primes. p_1. p_2. p_3. The processor **20** will develop the sub tasks identified above. using M. e. p_1 p_2. p_3 Thus. for example. if the exponentiator **32***a* were assigned the sub-task of developing C_1. the processor would develop the values M_1. e_1. and (p_1-1) and deliver units (write) these values. with n. to the exponentiator **32***a*. Similar values will be developed by the processor **20** for the sub-tasks that will be delivered to the exponentiators **32***b* and **32***c*.

In turn. the exponentiators **32** develop the values C_1. C_2. and C_3 which are returned to (retrieved by) the CPU **14**. The processor **20** will then combine the values C_1. C_2. and C_3 to form C. the ciphertext encryption of M. which is then returned to the host via the bus **12**.

The encryption. decryption techniques described hereinabove. and the use of the cryptosystem **10** (FIG. **1**) can find use in a number of diverse environments. Illustrated in FIG. **3** is one such environment. FIG. **3** shows a host system **50**. including the bus **12** connected to a plurality of cryptosystems **10** (**10***a*. **10***b*. . . . . **10***m*) structured as illustrated in FIG. **1**. and described above. In turn. the host system **50** connects to a communication medium **60** which could be. for example. an internet connection that is also used by a number of communicating stations **64**. For example. the host system **50** may be employed by a financial institution running a web site accessible. through the communication medium. by the stations **64**. Alternatively. the communication medium may be implemented by a local area network (LAN) or other type network. Use of the invention described herein is not limited to the particular environment in which it is used. and the illustration in FIG. **3** is not meant to limit in any way how the invention can be used.

As an example. the host system. as indicated. may receive encrypted communication from the stations **64**. via the communication medium **60**. Typically. the data of the communication will be encrypted using DES. and the DES key will be encrypted using a public key by the RSA scheme. preferably one that employs three or more distinct prime numbers for developing the public and private keys.

Continuing. the DES encrypted communication. including the DES key encrypted with the RSA scheme. would be received by the host system. Before decrypting the DES communication. it must obtain the DES key and. accordingly. the host system **50** will issue. to one of the cryptosystems **10** a decryption request instruction. containing the encrypted DES key as the cyphertext C. If the (private) decryption keys. d. n (and its component primes. $p_1 \cdot p_2 \cdot \ldots p_k$) are not held by the cryptosystem **10**. they also will be delivered with the encryption request instruction.

In turn. the cryptosystem **10** would decrypt the received cyphertext in the manner described above (developing the sub-tasks. issuing the sub-tasks to the exponentiator **32** of the cryptosystem **10**. and reassembling the results of the sub-task to develop the message data: the DES key). and return to the host system the desired. decrypted information.

Alternatively. the post-system **50** may desire to deliver. via the communication medium **60**. an encrypted communication to one of the stations **64**. If the communication is to be encrypted by the DES scheme. with the DES key encrypted by the RSA scheme. the host system would encrypt the communication. forward the DES key to one of the cryptosystems **10** for encryption via the RSA scheme. When the encrypted DES key is received back from the cryptosystem **10**. the host system can then deliver to one or more of the stations **64** the encrypted message.

Of course. the host system **50** and the stations **64** will be using the RSA scheme of public key encryption/decryption. Encrypted communications from the stations **64** to the host system **50** require that the stations **64** have access to the public key E (E. N) while the host system maintains the private key D (D. N. and the constituent primes. $p_1 \cdot p_2 \cdot \ldots \cdot p_k$). Conversely. for secure communication from the host system **50** to one or more of the stations **64**. the host system would retain a public key E' for each station **64**. while the stations retain the corresponding private keys E'.

Other techniques for encrypting the communication could used. For example. the communication could be entirely encrypted by the RSA scheme. If. however. the communication greater than n−1. it will need to be broken up into blocks size M where

$$0 \leqq M \leqq N-1$$

Each block M would be separately encrypted/decrypted. using the public key/private key RSA scheme according to that described above.

What is claimed:

1. A method for establishing cryptographic communications comprising the step of:

encoding a plaintext message word M to a ciphertext word signal C. where M corresponds to a number representative of a message and

$$0 \leqq M \leqq n-1$$

n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where k is an integer greater than 2. p_1. p_2. . . . p_k are distinct prime numbers. and where C is a number representative of an encoded form of message word M. wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby

$$C = M^e (\bmod n)$$

where e is a number relatively prime to $(p_1-1) \cdot (p_2-1)$.

2. The method according to claim **1**. comprising the further step of:

decoding the ciphertext word signal C to the message word signal M. wherein said decoding step comprises the step of: transforming said ciphertext word signal C. whereby:

$$M=C^d(\mathrm{mod}\ n)$$

where d is a multiplicative inverse of $e(\mathrm{mod}(\mathrm{lcm}((p_1-1).\ (p_2-1).\ \ldots .\ (p_k-1))))$.

3. A method for transferring a message signal M_i in a communications system having j terminals. wherein each terminal is characterized by an encoding key $E_i=(e_i.\ n_i)$ and decoding key $D_i=(d_i.\ n_i)$. where i=1. 2. . . . . j. and wherein M_i corresponds to a number representative of a message-to-be-transmitted from the i^{th} terminal. n_i is a composite number of the form

$$n_i=P_{i,1}\cdot p_{i,2}\cdot\ \ldots\ \cdot p_{i,k}$$

where k is an integer greater than 2.

$p_{i,1}.\ p_{i,2}.\ \ldots .\ p_{i,k}$ are distinct prime numbers.

e_i is relatively prime to $\mathrm{lcm}(p_{i,1}-1.\ p_{1,2}-1.\ p_{i,k}-1)$ d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i(\mathrm{mod}(\mathrm{lcm}((p_{i,1}-1).\ (p_{i,2}-1).\ \ldots .\ (p_{i,k}-1)))).$$

comprising the step of:

encoding a digital message word signal M_A for transmission from a first terminal (i=A) to a second terminal (i=B). said encoding step including the sub-step of:

transforming said message word signal M_A to one or more message block word signals M_A''. each block word signal M_A'' corresponding to a number representative of a portion of said message word signal M_A in the range $0\leqq M_A''\leqq n_B-1$.

transforming each of said message block word signals M_A'' to a ciphertext word signal C_A. C_A corresponding to a number representative of an encoded form of said message block word signal M_A''. whereby:

$$C_A\equiv M_A''^{e_B}(\mathrm{mod}\ n_B).$$

4. A cryptographic communications system comprising:

a communication medium:

an encoding means coupled to said channel and adapted for transforming a transmit message word signal M to a ciphertext word signal C and for transmitting C on said channel. where M corresponds to a number representative of a message and

$0\leqq M\leqq n-1$ where n is a composite number of the form

$$n=p_1\cdot p_2\ \ \cdot\ p_k$$

where k is an integer greater than 2 and $p_1.\ p_2.\ \ldots .\ p_k$ are distinct prime numbers. and where C corresponds to a number representative of an enciphered form of said message and corresponds to

$$C\equiv M^e(\mathrm{mod}\ n)$$

where e is a number relatively prime to $\mathrm{lcm}(p_1-1.\ p_2-1.\ \ldots .\ p_k-1)$: and

a decoding means coupled to said channel and adapted for receiving C from said channel and for transforming C to a receive message word signal M' where M' corresponds to a number representative of a deciphered form of C and corresponds to

$$M'\equiv C^{d}(\mathrm{mod}\ n)$$

where d is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e(\mathrm{mod}(\mathrm{lcm}((p_1-1),\ (p_2-1),\ \ldots,\ (p_k-1)))).$$

5. A cryptographic communications system having a plurality of terminals coupled by a communications channel. including a first terminal characterized by an associated encoding key $E_A=(e_A,\ n_A)$ and decoding key $D_A=(d_A,\ n_A)$. wherein n_A is a composite number of the form

$$n_A=p_{A,1}\cdot p_{A,2}\cdot\ \cdot p_{A,k}$$

where k is an integer greater than 2. $p_{A,1}$, $p_{A,2}$, ... $p_{A,k}$ are distinct prime numbers. e_A is relatively prime to

$$\mathrm{lcm}(p_{A,1}-1,\ p_{A,2}-1,\ \ldots,\ p_{A,k}-1),$$

d_A is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_A(\mathrm{mod}(\mathrm{lcm}((p_{A,1}-1),\ (p_{A,2}-1),\ \ldots,\ (p_{A,k}-1)))),$$

and including a second terminal. comprising:

blocking means for transforming a message-to-be-transmitted from said second terminal to said first terminal to one or more transmit message word signals M_B, where M_B corresponds to a number representative of said message in the range

$$0\leqq M_B\leqq n_A-1,$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B and for transmitting C_B on said channel,

where C_B corresponds to a number representative of an enciphered form of said message and corresponds to

$$C_B\equiv M_B^{eA}(\mathrm{mod}\ n_A)$$

wherein said first terminal comprises:

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_B from said channel and for transforming each of said ciphertext word signals to a receive message word signal M_B, and means for transforming said receive message word signals M' to said message. where M' is a number representative of a deciphered form of C_B and corresponds to

$$M_B'\equiv C_B^{da}(\mathrm{mod}\ n_A).$$

6. The system according to claim 5 wherein said second terminal is characterized by an associated encoding key $E_B=(e_B,\ n_B)$ and decoding key $DB=(D_B,\ d_B)$, where:

n_B is a composite number of the form

$$n_B=p_{B,1}\ p_{B,2}\cdot\ \ \ p_{B,k}$$

where k is an integer greater than 2. $p_{B,1}$, $p_{B,2}$, ... $p_{B,k}$ are distinct prime numbers. e_B is relatively prime to

$$\mathrm{lcm}(p_{B,1}-1,\ p_{B,2}-1,\ \ldots,\ p_{B,k}-1),$$

d_B is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_B(\mathrm{mod}(\mathrm{lcm}((p_{B,1}), (p_{B,2}-1), \ldots, (p_{B,k}-1)))),$$

wherein said first terminal comprises:

blocking means for transforming a message-to-be-transmitted from said first terminal to said second terminal. to one or more transmit message word signals M_A. where M_A corresponds to a number representative of said message in the range

$$0 \leqq M_A{}^{eB}(\mathrm{mod}\ n_B)$$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel.

where C_A corresponds to a number representative of an enciphered form of said message and corresponds to

$$C_A \equiv M_A{}^{eB}(\mathrm{mod}\ n_B)$$

wherein said second terminal comprises;

decoding means coupled to said channel and adapted for receiving said ciphertext word signals C_A from said channel and for transforming each of said ciphertext word signals to a receive message word signal M_A'. and means for transforming said receive message word signals M_A to said message.

where M' corresponds to a number representative of a deciphered form of C and corresponds to

$$M_A' \equiv C_A{}^{dB}(\mathrm{mod}\ n_B).$$

7. A method for establishing cryptographic communications comprising the step of:

encoding a digital message word signal M to a cipher text word signal C. where M corresponds to a number representative of a message and

$$0 \leqq M \leqq n-1,$$

where n is a composite number having at least 3 whole number factors greater than one. the factors being distinct prime numbers. and

where C corresponds to a number representative of an encoded form of message word M.

wherein said encoding step comprises the step of:

transforming said message word signal M to said ciphertext word signal C whereby

$$C \equiv c_e M^e + a_{e-1} M^{e-1} + . \quad + a_0(\mathrm{mod}\ n)$$

where e and a_e. a_{e-1}. . . . . a_0 are numbers.

8. In the method according to claim 7 where said encoding step includes the step of transforming M to C by the performance of a first ordered succession of invertible operations on M. the further step of:

decoding C to M by the performance of a second ordered succession of invertible operations on C. where each of the invertible operations of said second succession is the inverse of a corresponding one of said first succession. and wherein the order of said operations in said second succession is reversed with respect to the order of corresponding operations in said first succession.

9. A communication system for transferring message signals M_i, comprising:

j stations, each of the j stations being characterized by an encoding key $E_i=(e_i, n_i)$ and decoding key $D_i=(d_i, n_i)$, where i=1,2, . . . , j, and wherein

M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal, and

$$0 \leqq M_i \leqq n_i - 1,$$

n_i is a composite number of the form

$$n_i = pi_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$$

where k is an integer greater than 2,

$p_{i,1}$, $p_{i,2}$, . . . , $p_{i,k}$ are distinct prime numbers,

e_i is relatively prime to lcm($p_{i,1}-1$,$p_{i,2}-1$, . . . , $p_{i,k}-1$),

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i(\mathrm{mod}(\mathrm{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))));$$

a first one of the j terminals including

means for encoding a digital message word signal M_A for transmission from said first terminal (i=A) to a second one of the j terminals (i=B), and

means for transforming said message word signal M_A to a signed message word signal M_{As}, M_{As} corresponding to a number representative of an encoded form of said message word signal M_A, whereby:

$$M_{As} \equiv M_A^{dA} (\mathrm{mod}\ n_A).$$

10. The system of claim 9 further comprising:

means for transmitting said signal message word signal M_{As} from said first terminal to said second terminal, and wherein said second terminal includes means for decoding said signed message word signal M_{As} to said message word signal M_A, said second terminal including:

means for transforming said signed message word signal M_{AS} to said message word signal M_A, whereby

$$M_A \equiv M_{As}^{eA} (\mathrm{mod}\ n_A).$$

11. A communications system for transferring a message signal M_i, the communications system comprising

j communication stations each characterized by an encoding key $E_i=(e_i, n_i)$ and decoding key $D_i=(d_i, n_i)$, where i=1, 2, . . . , j, and wherein M_i corresponds to a number representative of a message signal to be transmitted from the i^{th} terminal, n_i is a composite number of the form

$$n_i = p_{i,1} \, p_{i,2} \cdot \; \cdot \; p_{i,k}$$

where

k is an integer greater than 2,

$p_{i,1}$, $p_{i,2}$, . . . , $p_{i,k}$ are distinct prime numbers,

e_i is relatively prime to lcm($p_{i,1}-1$,$p_{i,2}-1$, . . . , $p_{i,k}-1$),

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$$e_i(\mathrm{mod}(\mathrm{lcm}((p_{i,1}-1).\ (p_{i,2}-1).\ .\quad .\ (p_{i,k}-1))))$$

a first one of the j communication stations including

means for encoding a digital message word signal M_A for transmission from said first one of the j communication stations (i=A) to a second one of the j communication stations (i=B).

means for transforming said message word signal M_A to one or more message block word signals M_A". each block word signal M_A' being a number representative of a portion of said message word signal M_A' in the range $0 \leqq M_A \leqq n_B-1$. and

means for transforming each of said message block word signals M_A" to a ciphertext word signal C_A. C_A corresponding to a number representative of an encoded form of said message block word signal M_A". whereby:

$$C_A \equiv M_A{}^{"Eb}(\mathrm{mod}\ n_B).$$

12. The system of claim 11 further comprising:

means for transmitting said ciphertext word signals from said first terminal to said second terminal. and

wherein said second terminal includes means for decoding said ciphertext word signals to said message word signal MA. said second terminal including:

means for transforming each of said ciphertext word signals C_A to one of said message block

word signals M_A". whereby

$$M_A'' \equiv C_A^{Db} (\mathrm{mod}\ n_B)$$

means for transforming said message block word signals M_A" to said message word signal M_A.

13. In a communications system, including first and second communicating stations interconnected for communication therebetween.

the first communicating station having

encoding means for transforming a transmit message word signal M to a ciphertext word signal C where M corresponds to a number representative of a message and

$$0 \leqq M \leqq n-1$$

where n is a composite number having at least 3 whole number factors greater than one. the factors being distinct prime numbers. and

where C corresponds to a number representative of an enciphered form of said message and corresponds to

$$C \equiv a_e M^e + a_{e-1} M^{e-1} + \ .\ .\ + a_0 (\mathrm{mod}\ n)$$

where e and a_e. a_e−1. . . . . a_0 are numbers: and means for transmitting the ciphertext word signal C to the second communicating station.

* * * * *